28

giugno 2006

i Quaderni

sommario

Linee guida alla continuità operativa nella Pubblica Amministrazione

i Quaderni n. 28 giugno 2006
Supplemento al n. 10/2006
del periodico "InnovAzione"

Registrato al Tribunale di Roma
n. 523/2003
del 15 dicembre 2003

Direttore responsabile
Franco Tallarita
tallarita@cnipa.it

Quaderno a cura
di Gaetano Santucci
continuita_operativa@cnipa.it

Redazione
Centro Nazionale
per l'Informatica nella
Pubblica Amministrazione
Via Isonzo, 21b
00198 Roma
Tel. 06 85264.1

I Quaderni
del Cnipa sono pubblicati
all'indirizzo:
www.cnipa.gov.it

Stampa:
Stabilimenti Tipografici
Carlo Colombo S.p.A. – Roma

Prefazione

La Pubblica Amministrazione deve assicurare la continuità dei propri servizi per garantire il corretto svolgimento della vita nel Paese, anche in presenza di eventi imprevisti, ai quali si è finora fatto fronte, generalmente, ricorrendo a soluzioni di emergenza di tipo tradizionale (spostamento di personale tra uffici, attivazione di procedure manuali in sostituzione di quelle informatizzate temporaneamente sospese, ecc.).
La crescita progressiva dell'utilizzo delle tecnologie informatiche rende il problema della continuità dei servizi più complesso. Ormai la quasi totalità dei procedimenti amministrativi basa almeno una fase del proprio iter su sistemi e applicazioni informatiche. Pertanto gli inconvenienti di natura tecnica possono portare all'interruzione totale dei servizi istituzionali anche per lunghi periodi, e non appare possibile annullare o mitigare gli effetti negativi di un'interruzione del funzionamento dei sistemi informatici esclusivamente con procedure manuali alternative e strumenti tradizionali.
Il tema della continuità operativa (l'espressione "continuità operativa" può essere considerata come la trasposizione italiana delle espressioni *disaster recovery* e *business continuity*) riguarda l'insieme dei metodi e degli strumenti finalizzati ad assicurare la continuità dei servizi istituzionali anche in presenza di eventi indesiderati che possono causare il fermo prolungato dei sistemi informatici. Si osserva che le soluzioni per garantire la continuità dei servizi non considerano soltanto le componenti tecnologiche utilizzate ma anche tutte le altre risorse (personale, impianti, ecc.). La continuità operativa considera i mezzi tecnici impiegati nei procedimenti amministrativi come strumenti per l'erogazione dei servizi ed estende la sua sfera di interesse alle tematiche più generali di natura organizzativa.
Da tempo il CNIPA si è fatto carico di seguire e promuovere la continuità operativa nel settore pubblico, anche attraverso la costituzione di un centro di competenza, cui sono stati invitati a partecipare le pubbliche amministrazioni centrali e locali, i rappresentanti dei fornitori ed altri soggetti istituzionali interessati. Questo documento di indirizzo è il frutto degli incontri e dei lavori che, in tale ambito, si sono svolti sul tema della continuità operativa e rappresenta un'utile guida per le amministrazioni che devono soddisfare il requisito della continuità dei servizi istituzionali.
Si ringraziano tutti coloro che hanno partecipato al Gruppo di Lavoro che ha consentito la realizzazione di questo importante risultato ed in particolare:

Stefano APRILE	Ministero giustizia
Annarita BOVE	MIUR
Giuseppe CONCORDIA	MEF
Renzo FERRUCCI	INPS
Francesco GRASSO	CNIPA

Antonio LACENTRA	Regione Veneto
Mariano LUPO	MEF
Giuseppe NERI	AITech-Assinform
Daniele PERUCCHINI	Ministero comunicazioni
Giancarlo PONTEVOLPE	CNIPA
Giovanni RELLINI LERZ	CNIPA
Gaetano SANTUCCI (coordinatore)	CNIPA
Romano STASI	ABI Lab
Stefano VENANZI	CNIPA
Raffaele VISCIANO	MEF

Hanno poi fattivamente collaborato alcune Imprese associate ad AITech-Assinform che, chiamate a questo impegno da detta Associazione, hanno risposto dando un significativo contributo al lavoro tramite la partecipazione di circa 25 dipendenti.

CA Technology Service
Cisco Systems Italy
EDS
EMC Computer Systems Italia
Engineering Ingegneria Informatica
Finsiel - Gruppo Alma Viva
Getronics
Hewlett Packard
IBM Italia
Micro Focus
Nortel
Oracle
Siemens Informatica
Theorematica

Un particolare ringraziamento va pertanto a:

Fabio Berno
Luciano Boschetti
Gianluca De Risi
Sandro De Santis
Marco Falchi
Fabrizio Gergely
Maurizio Giovannetti
Matteo La Speme
Nando La Volpe
Pier Luigi Grassi
Lucilla Mancini
Nicola Marrucci
Marco Marzi Marchesi
Lucio Micheli
Roberto Missana
Ombretta Palma
Fausto Pompei
Sergio Resch
Fabrizio Ricelli
Orsio Romagnoli
Felice Santosuosso
Marco Schina
Isabella Taschetta
Alfredo Valenza
Maurizio Viziano
Roberto Zollo

Claudio Manganelli
Componente del Collegio CNIPA

Linee guida alla continuità operativa
nella Pubblica Amministrazione

Obiettivi e scenari della continuità operativa delle pubbliche amministrazioni

Il presente documento tratta del tema della continuità operativa nelle amministrazioni pubbliche, intendendo con tale espressione l'insieme dei metodi e degli strumenti finalizzati ad assicurare la continuità dei servizi istituzionali anche in presenza di eventi indesiderati che possono causare il fermo prolungato dei sistemi informatici.
Si osserva, a tal proposito, che la Pubblica Amministrazione è tenuta ad assicurare la continuità dei propri servizi per garantire il corretto svolgimento della vita nel Paese[1].
Quest'obbligo finora è stato assolto, anche in presenza di eventi imprevisti, ricorrendo a soluzioni di emergenza di tipo tradizionale quali: il trasferimento dei servizi presso gli uffici rimasti operativi, l'attivazione di procedure amministrative alternative, l'ausilio di personale aggiuntivo, ecc. Oggi l'impiego di procedure alternative di tipo tradizionale è quasi sempre insufficiente a garantire la continuità dei servizi, per il diffuso utilizzo delle tecnologie informatiche. Infatti, anche quando il procedimento amministrativo sembra essere "non informatizzato", sicuramente almeno una fase del suo iter necessita di applicazioni informatiche, pertanto inconvenienti di natura tecnica possono condizionare il normale svolgimento dei processi tradizionali fino a comportare il blocco delle attività istituzionali anche per lunghi periodi.
Da quanto detto consegue che la continuità dei servizi informatici rappresenta un impegno inderogabile per la Pubblica Amministrazione che dovrà operare in modo da limitare al massimo gli effetti negativi di possibili fermi prolungati dei servizi ICT.
Relativamente alle cause che possono compromettere la continuità di un sistema informatico, possiamo distinguere le seguenti categorie:

a) problemi di funzionamento, dovuti ad errori di progettazione, di configurazione o di esercizio dei diversi prodotti hardware e software che costituiscono il sistema informatico;
b) eventi di tipo accidentale o malevolo, in grado di inficiare la continuità operativa di alcune applicazioni per un periodo di tempo limitato (minuti-ore);
c) danni dovuti a cause impreviste, difficilmente fronteggiabili, che possono comportare l'indisponibilità delle funzioni informatiche per un periodo di tempo consistente (giorni-mesi).

Anche se la soluzione per queste diverse tipologie di problemi è spesso comune, è prassi classificare, comunque, in modo diverso le relative problematiche:

- la gestione dei problemi di tipo a) rientra nel tema della qualità dei prodotti e dei servizi informatici;

[1] Si ricorda l'art. 97 della Costituzione ed il principio di buon andamento dell'amministrazione da rispettare anche se si utilizzano tecnologie ICT.

- gli episodi di tipo b) sono normalmente trattati nell'ambito delle attività relative alla sicurezza informatica;
- i casi di cui al punto c) afferiscono invece alle discipline comunemente note come *disaster recovery* e *business continuity*.

Le espressioni *disaster recovery* e *business continuity* sono usate con varie accezioni e, talvolta, come sinonimi. L'uso più diffuso definisce come *disaster recovery* le attività necessarie per ripristinare – in tutto o in parte – le funzionalità del sistema informatico inteso come complesso di strutture hardware, software e servizi di comunicazione, mentre il termine *business continuity* si riferisce ai metodi che consentono di eliminare o ridurre gli effetti negativi di situazioni disastrose assicurando la continuità dei servizi di impresa o istituzionali[2].

Sebbene le problematiche di tipo a) e b) possano ricadere anche in altre discipline, l'argomento della continuità operativa comprende, per definizione, tutte le casistiche esposte. Infatti qualunque problema che assuma una rilevanza straordinaria deve essere affrontato con metodi e tecniche particolari che ricadono nelle pratiche di "continuità operativa".

Qualche esempio potrà chiarire meglio questo aspetto. Un problema hardware è un evento ordinario che viene di solito gestito secondo quanto previsto dalle procedure di manutenzione con livelli di servizio commisurati all'impiego dell'apparato. Un guasto hardware può causare una discontinuità operativa ma, quando il periodo di interruzione rientra nei parametri di qualità del servizio, tale evento viene considerato normale e non provoca l'innesco del piano di continuità operativa. Può accadere però che, per motivi imprevisti (ad esempio per irreperibilità di una parte di ricambio), il periodo di interruzione sia superiore a quello accettabile secondo i parametri di qualità del servizio. In tale evenienza, anche se la causa del problema è un evento ordinario, è opportuno gestire la circostanza particolare secondo le modalità descritte nel presente documento, ossia con i metodi e le tecniche della continuità operativa. Analogamente, se un problema di sicurezza determina un'interruzione del servizio di durata eccessiva, può essere opportuno avviare le procedure di continuità operativa per garantire che l'interruzione rimanga entro limiti tollerabili.

Occorre osservare che tra gli eventi elencati sussiste una differenza che condiziona alquanto gli approcci alla continuità operativa.

Gli eventi di tipo calamitoso (incendi, allagamenti, ecc.) si manifestano subito nella loro gravità e dunque comportano senz'altro la partenza del piano di continuità operativa.

I problemi di qualità e di sicurezza si manifestano invece inizialmente come problemi ordinari e solo a seguito di ripetuti insuccessi delle procedure abituali di recupero assumono la consistenza dei problemi di continuità operativa. Infatti la gravità del problema può aumentare progressivamente nel tempo senza che sia possibile determinare in anticipo il livello di criticità che assumerà l'evento. Ciò comporta la necessità di stabilire, volta per volta, se sia il caso o meno di avviare le procedure di continuità operativa e questa decisione sarà tanto più critica quanto maggiori saranno i costi per l'avvio del piano di continuità operativa ed il rientro alla normalità.

[2] L'espressione "business continuity" (continuità dell'impresa) richiama il mondo industriale ma, riferendoci al settore pubblico, nel seguito del documento useremo tale espressione per indicare la continuità dei procedimenti amministrativi e dei servizi istituzionali.

Il confine tra le procedure per la qualità dei servizi, la sicurezza e la continuità operativa è alquanto sottile e soggettivo. Alcuni tendono a considerare questi aspetti come parte di un unico problema che deve essere gestito in modo unitario ed integrato, altri separano la gestione dei problemi ordinari (qualità e sicurezza) da quelli calamitosi (*disaster recovery-business continuity*).
Nel seguito del documento seguiremo il secondo approccio, trattando essenzialmente le problematiche relative alla gestione della continuità nel caso di eventi di natura eccezionale e rimandando ad altre linee guida la gestione della qualità e della sicurezza[3]. Ciò nondimeno saranno evidenziati i casi in cui i metodi o le soluzioni di continuità operativa possono essere di ausilio anche per le procedure di qualità e di sicurezza del sistema informatico.

[3] Si vedano i quaderni del CNIPA relativi alla qualità (n. 10-13) ed alla sicurezza (n. 23).

Breve guida alla lettura

Il capitolo 1 illustra i metodi con cui è possibile affrontare il tema della continuità operativa, delineando il percorso per la scelta della soluzione ottimale, la pianificazione degli interventi di recupero e la progettazione e realizzazione delle iniziative volte a migliorare la capacità di risposta a problemi che possono compromettere la continuità delle attività istituzionali.
Il capitolo 2 tratta l'argomento della continuità operativa sotto l'aspetto economico, stimando i costi che possono essere causati da fermi prolungati dei servizi istituzionali ed i vantaggi derivanti dalla pianificazione di interventi per la continuità dei medesimi. Nel capitolo viene anche proposto un esempio di raffronto tra costi e benefici al variare della tipologia di soluzione di continuità operativa adottata.
Il capitolo 3 costituisce una guida sulle modalità con cui affrontare il problema della continuità operativa sotto l'aspetto organizzativo. In particolare vengono fornite indicazioni su come impostare il progetto affinché l'obiettivo della continuità dei servizi possa essere raggiunto efficacemente e mantenuto nel tempo al variare delle condizioni al contorno.
Il capitolo 4 analizza l'argomento della continuità operativa evidenziando le opzioni ed i vincoli previsti dalla normativa vigente ed illustrando, anche con esempi, le soluzioni contrattuali che possono essere intraprese dalla Pubblica Amministrazione. Sono presenti anche alcuni spunti per la definizione di forme associative tra amministrazioni che consentono il contenimento dei costi (accordi di mutuo soccorso, convenzioni, consorzi, centri di backup comuni, ecc.).
Nel capitolo 5 viene proposta una rassegna delle tecnologie usualmente impiegate per migliorare la continuità dei servizi e per rendere efficienti le attività di ripristino dell'operatività a seguito di un evento imprevisto.
Il documento è completato da alcune appendici in cui sono proposti schemi di documenti di analisi e pianificazione, nonché modelli contrattuali.
È possibile trovare una sintesi del presente documento nel "Quadernino" CNIPA n. 10 che illustra i concetti principali della continuità senza entrare nel merito delle specifiche soluzioni.

1. Aspetti metodologici

Nell'accezione di questo documento, il termine "metodologia" indica un insieme strutturato di attività che, condotte in un dato ordine, definiscono un percorso che porta a un obiettivo prefissato. In questo capitolo verranno illustrati i passi di un possibile percorso attraverso il quale una pubblica amministrazione può studiare, progettare e realizzare una soluzione di continuità operativa adeguata alle proprie esigenze.
Nella definizione di questo percorso, si farà nel seguito ampio riferimento alle metodologie, alle tecniche e ai termini reperibili nella letteratura tecnica (studi, rapporti di analisti, opinioni di esperti, documentazione di fornitori di tecnologia e servizi) esistente sull'argomento, calando però – quanto più possibile – i concetti generali nella realtà specifica della Pubblica Amministrazione italiana. Di tutti i concetti trattati verrà data una definizione, esempi, best practice, indicazioni e consigli.
Questo capitolo tratta la questione della scelta della soluzione principalmente sotto l'aspetto tecnico-organizzativo. Il capitolo successivo approfondirà la valutazione degli aspetti economici della soluzione.
Non è scopo di questo documento identificare o raccomandare un'unica metodologia per gestire tutti i problemi di continuità operativa ipotizzabili nel contesto della Pubblica Amministrazione, ma fornire alle amministrazioni più strumenti metodologici, anche alternativi tra loro, che potranno essere utili per affrontare l'argomento.
Non tutti i passi metodologici descritti nel seguito sono indispensabili per progettare e realizzare correttamente una soluzione di continuità. A seconda delle caratteristiche e del contesto della singola amministrazione, alcuni passi potrebbero essere superflui, o da condurre solo per grandi linee, in quanto l'impegno richiesto per la loro esecuzione potrebbe non essere giustificato dai benefici ottenibili.
In ogni caso, una conoscenza del percorso completo è necessaria per identificare quali passi – nei vari casi – siano indispensabili e quali invece possano essere tralasciati.
L'obiettivo finale da raggiungersi attraverso passi intermedi che possono essere diversi a seconda del percorso intrapreso, è generalmente una soluzione tecnico-organizzativa in grado di soddisfare le esigenze di continuità esistenti.
Alcune metodologie, in realtà, giungono soltanto fino alla determinazione della soluzione migliore (o, meglio, più adeguata alle esigenze) ed alla stima di impegno economico per la realizzazione della soluzione stessa. In questo documento, viceversa, faremo rientrare nel percorso metodologico anche la fase di realizzazione, di gestione e di manutenzione della soluzione.
La figura che segue riassume le fasi previste dalla quasi totalità delle metodologie esistenti: il percorso (circolare, in quanto si tratta di un processo continuo) prevede, dopo la fase iniziale di studio/analisi del contesto, il conseguente disegno della soluzione tecnologica e organizzativa che meglio risponde alle esigenze di continuità richieste, e infine la realizzazione e il mantenimento della soluzione.
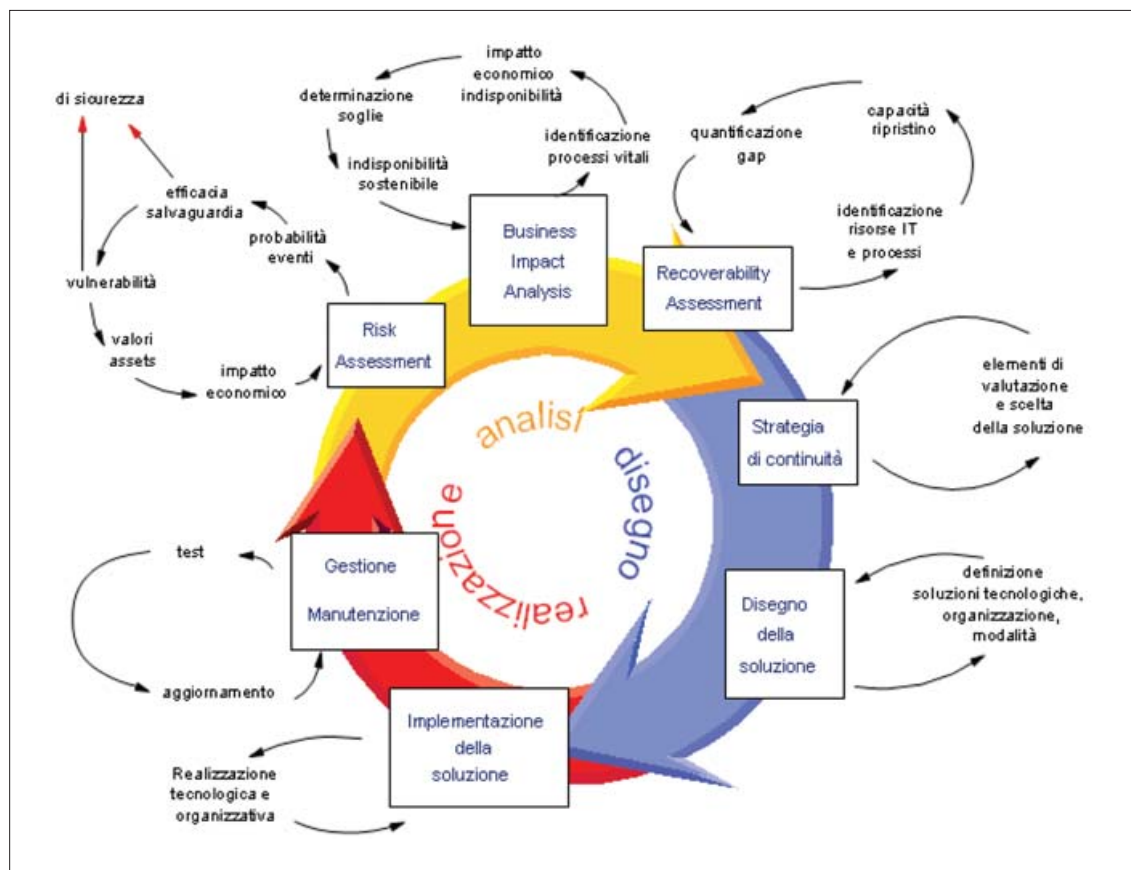
Figura 1

1.1 STUDIO/ANALISI DEL CONTESTO

Tutti i percorsi metodologici esistenti nella letteratura tecnica hanno come punto di partenza lo studio del contesto di riferimento, cioè del quadro tecnologico e organizzativo all'interno del quale esiste un'esigenza di continuità operativa da soddisfare: del resto, fa parte del buonsenso comune l'idea che per ottenere una buona soluzione dei propri problemi, questi ultimi vadano anzitutto compresi al meglio.
Come mostra la figura precedente, lo studio/analisi del contesto si può suddividere nelle sottofasi di *Risk Assessment, Business Impact Analysis* e *Recoverability Assessment.*
In generale, lo studio del contesto è indirizzato a stabilire la tipologia di eventi dalla quale l'amministrazione intende proteggersi: una corretta identificazione degli eventi d'interesse permette di restringere in anticipo la scelta tra le soluzioni utili per eliminare o mitigare gli effetti degli eventi stessi.
All'interno dell'insieme di tutti i possibili eventi, nel seguito sarà posta particolare attenzione agli eventi che interrompono l'erogazione dei servizi di pertinenza dell'amministrazione a causa dell'indisponibilità prolungata del sistema informatico. Una possibile classificazione di tali eventi è la seguente:

- eventi pianificati (es.: manutenzione degli impianti tecnologici, aggiornamento di componenti, lavori di ristrutturazione della sede, ecc...);

- eventi non pianificati (incidenti, guasti all'alimentazione elettrica, cadute della rete, malfunzionamenti, ecc…), in grado di causare indisponibilità prolungata dei servizi.

Ogni evento è caratterizzato da:

- una frequenza d'accadimento;
- la durata (ove applicabile);
- l'impatto che causa sui servizi erogati dall'amministrazione[4].

Tipicamente, le soluzioni di continuità prendono in considerazione l'effetto di un evento e non le sue cause. Al contrario, la prevenzione degli eventi è generalmente demandata a forme di intervento (quali, ad esempio, l'adozione di misure per la sicurezza e integrità fisica degli impianti) non classificabili come "soluzioni di continuità".
La figura seguente propone un confronto tra eventi pianificati e non pianificati, riportando alcune delle cause che possono provocare impatti sulla normale operatività di un'amministrazione. Nella stessa figura sono indicate, a titolo di esempio, alcune discipline e soluzioni adatte a fronteggiare le varie tipologie di eventi.
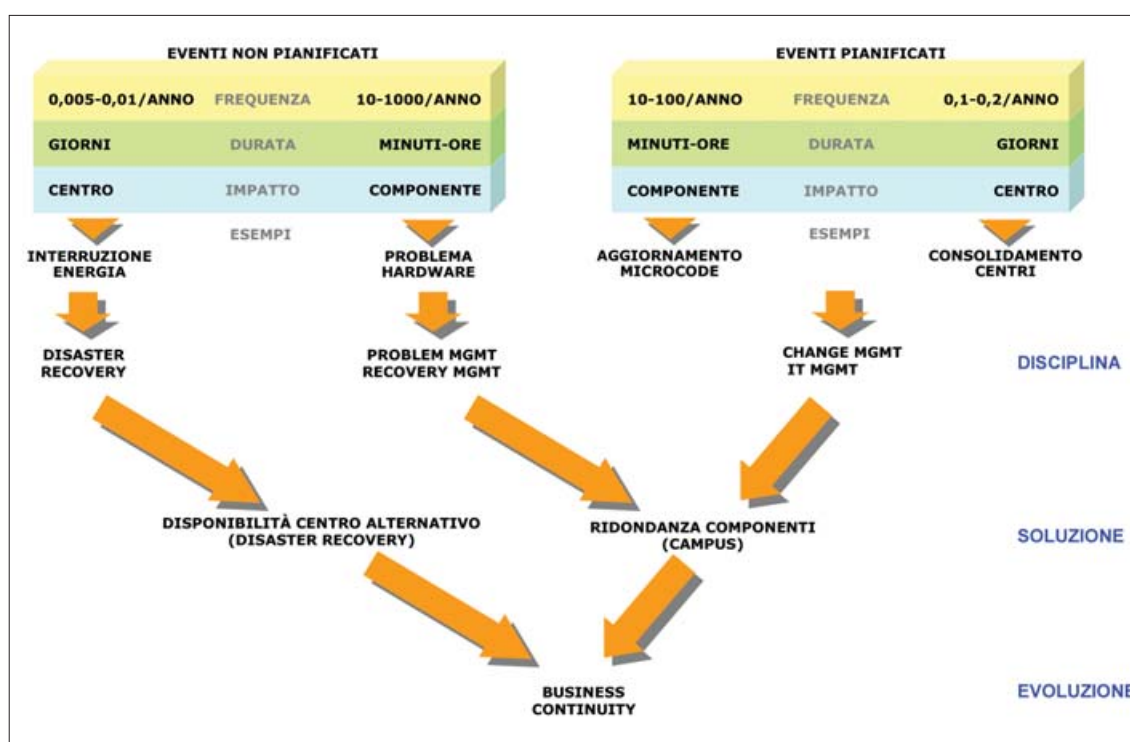
Figura 2

Assieme all'identificazione degli eventi da cui proteggersi, in questa fase si determina il perimetro entro il quale studiare le esigenze di continuità, cioè le strutture e i processi necessari alla continuità del servizio, le risorse tecnologiche (hardware, software, rete) e l'organizzazione (dipendenti, fornitori) a supporto di tali processi.

[4] È più significativo parlare di "impatto" di un evento che di sua "gravità". Tuttavia, i due concetti sono legati, in quanto un evento è tanto più grave quanto più esso impatta sui servizi erogati dall'amministrazione.

Ricapitolando, studiare il contesto significa analizzare:

- cosa proteggere;
- da quali eventi indesiderati;
- con quali livelli di servizio.

Cosa proteggere
Per identificare cosa proteggere, l'amministrazione deve censire i servizi erogati, identificando, tra questi, i servizi critici, cioè quei servizi che – per norma, missione istituzionale o altro – devono essere necessariamente mantenuti in operatività.
A volte un servizio può rivelarsi critico anche se l'amministrazione che lo eroga non è direttamente interessata a mantenerne l'operatività ed a proteggerlo. Può verificarsi infatti il caso che un servizio non sia critico per l'amministrazione che lo eroga, ma lo sia per un'altra amministrazione, "utente" della prima (vedi figura seguente). In questo caso, la prima amministrazione potrebbe decidere che tale servizio debba comunque essere incluso in quelli da proteggere.
Esempi di servizi erogati da un'amministrazione sono:

- rilascio (predisposizione e stampa) di un certificato anagrafico a un cittadino;
- prenotazione di una visita medica presso una struttura sanitaria;
- concessione di un'autorizzazione a un'azienda;
- invio dello stipendio a un dipendente pubblico (si noti che anche il dipendente è un "fruitore" dei servizi di un'amministrazione).

L'identificazione dei servizi erogati da un'amministrazione non è, generalmente un compito agevole. Un buon punto di partenza è l'elenco dei "procedimenti" che sono di competenza dell'amministrazione, in genere definiti da norme. Occorre ricordare che da un procedimento scaturisce un "servizio" ogni qualvolta il procedimento prevede un'interazione tra l'amministrazione e un utente esterno (che può essere un cittadino, un dipendente, un'impresa o un'altra amministrazione).
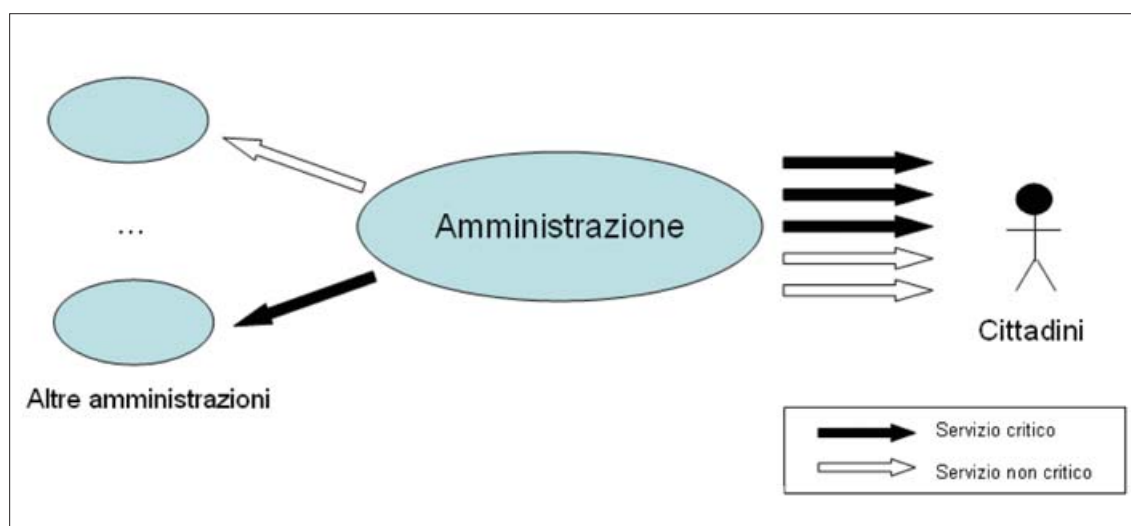
Figura 3

Per ogni servizio da proteggere, l'amministrazione deve identificare l'insieme delle risorse (umane, tecnologiche, procedurali e gli spazi di lavoro) necessarie alla sua erogazione. Tale insieme viene, in alcune metodologie, definito "isola". Nel seguito, per comodità, useremo ancora questa definizione, rappresentata graficamente nella figura seguente.
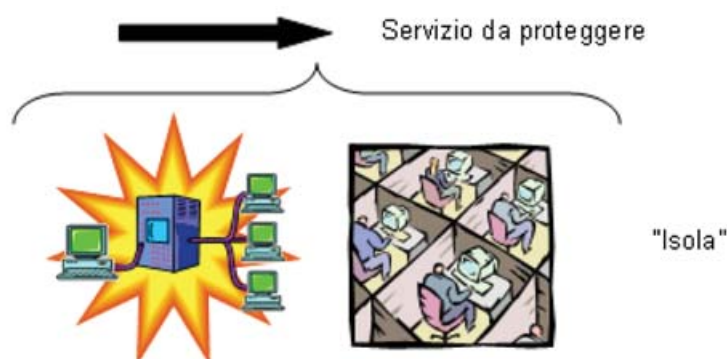
Figura 4

Un esempio di "isola" potrebbe essere l'insieme costituito da un sistema server, un apparato di stampa, una porzione di LAN, alcune postazioni di lavoro, i dipendenti di una specifica unità organizzativa, i locali di un ufficio.
Nell'identificare le risorse da proteggere, si deve tener conto anche di alcune tipologie di oggetti che non è intuitivo collegare direttamente a uno specifico servizio. Ad esempio:

- documenti di tipo contrattuale (con fornitori, assicurazioni, partner, ecc.);
- documentazione operativa (manuali, agende, guide, mappe, schemi tecnici, liste di password, configurazioni di sistema);
- materiale minuto vario (carte di credito, contante, assegni, timbri e sigilli amministrativi).

Da quali eventi

Nell'identificazione degli eventi da prendere in considerazione, va posta particolare attenzione agli eventi "non pianificati", perché sono generalmente la causa principale di interruzione della continuità operativa.
Può essere utile suddividere gli eventi non pianificati in due tipologie:

- "eventi fisici", cioè problemi su risorse infrastrutturali e tecnologiche; spaziano dai malfunzionamenti hardware (problematiche di componente) fino all'indisponibilità prolungata della sede che ospita l'ambiente considerato;
- "eventi logici", cioè problemi causati dal software, quali errori applicativi, virus informatici o attacchi da parte di hacker.

Gli eventi del primo tipo ricadono propriamente nel tema della continuità operativa. Viceversa, gli eventi logici sono quasi sempre affrontati e risolti tramite soluzioni di altro tipo, quali, ad esempio, politiche di *application management* o di *security management*.

Con quali livelli di servizio

Per ogni servizio da proteggere, è necessario determinare in che misura esso deve essere mantenuto in operatività. Tale misura viene in genere data attraverso i due indicatori

Recovery Time Objective (RTO, massimo tempo di indisponibilità del servizio, ovvero tempo entro il quale il servizio da proteggere deve essere ripristinato) e *Recovery Point Objective* (RPO, perdita dati sostenibile, in termini di distanza temporale tra il verificarsi dell'emergenza e l'ultimo salvataggio utile e ripristinabile dei dati).
La determinazione del RTO e del RPO dei servizi da proteggere viene in genere effettuata durante la *Business Impact Analysis* (vedi paragrafo 1.1.2).
I livelli di servizio sono normalmente diversi per i vari servizi da proteggere. Da ciò deriva il fatto che le esigenze di continuità di un'amministrazione sono, in generale, soddisfatte da un insieme di soluzioni tecnico-organizzative, piuttosto che da una sola. Ad esempio, possono essere realizzate soluzioni che assicurano una perdita dati prossima a zero per tutti quei servizi per i quali non è possibile o difficilmente realizzabile la ricostruzione o re-immissione dei dati, mentre per altri servizi (ad esempio il datawarehouse) possono essere attuate soluzioni meno impegnative e costose, perché i dati sono generalmente ricostruibili a partire da altri archivi.
Nella letteratura tecnica vi sono alcune proposte di classificazione dei servizi sulla base di RTO e RPO. Ad esempio, Gartner Group propone di classificare i servizi erogati in questo modo:

- servizi di classe 1: con RTO e RPO prossimi a zero;
- servizi di classe 2: con RTO dell'ordine delle 24 ore, e RPO prossimo a 4 ore;
- servizi di classe 3: con RTO dell'ordine delle 72 ore, e RPO prossimo a 24 ore;
- servizi di classe 4: con RTO misurabile in giorni, e RPO superiore a 24 ore.

I servizi delle prime due classi sono, in generale, quelli definibili "critici". Quelli appartenenti alla terza e quarta classe possono essere protetti anche con soluzioni non appartenenti all'area della continuità operativa (ad esempio semplicemente con un sistema di backup).
Nello studio del contesto vi sono altri aspetti che devono essere considerati: ad esempio si dovrà stabilire in anticipo l'eventuale degrado di prestazioni o aumento dei tempi di risposta nei servizi accettabili in caso di emergenza, così come i rischi residui verso i quali l'amministrazione potrebbe continuare ad essere esposta nonostante l'adozione di una soluzione di continuità. Infatti non tutti i rischi sono eliminabili, sia perché non economicamente conveniente sia perché si è disposti ad accettare gli effetti, dopo averli valutati, che ne potrebbero conseguire. Questa valutazione viene effettuata durante le fasi descritte nei prossimi due paragrafi.

1.1.1 Risk assessment

In questa fase (chiamata anche in letteratura tecnica "analisi del rischio") vanno determinati, analizzati e classificati i rischi a cui è soggetta l'amministrazione, e vanno stimate le vulnerabilità dell'amministrazione, in modo che quest'ultima sia poi capace di individuare le salvaguardie più adeguate ed efficaci.
Prima di tutto, è indispensabile definire gli oggetti cardine della problematica, fornendo definizioni sulle quali esiste, nella letteratura tecnica, un intendimento comune. Nel glossario allegato al presente documento sono presenti le definizioni di "rischio", "minaccia", "vulnerabilità" e "salvaguardia". Nel seguito si farà ampio riferimento a tali definizioni, eventualmente

estendendole, ove necessario. Alcuni concetti che verranno qui approfonditi sono già stati citati nel precedente paragrafo: ciò rispecchia l'approccio generale del presente documento, che consente una lettura a più livelli di approfondimento, con possibilità di fermarsi quando si ritiene di aver colto informazioni già sufficienti alla propria situazione.
Esistono due approcci principali per svolgere l'analisi del rischio. Il primo è marcatamente concettuale, indirizzato al management, orientato ai processi e all'organizzazione, e consegue l'obiettivo di aumentare la consapevolezza dei vertici dell'amministrazione sull'importanza di realizzare un piano di sicurezza con una visione più completa possibile.
Il secondo approccio è prettamente operativo, orientato agli specialisti, e consegue l'obiettivo di dettagliare e approfondire la sicurezza delle singole tecnologie.
Tra questi due approcci, quello da adottare va scelto volta per volta, sulla base del livello di approfondimento necessario, dei sistemi di misura utilizzati e della frequenza del processo di analisi (si noti che il processo va comunque ripetuto nel tempo).

Sistemi di misura

Rischio, minaccia e vulnerabilità sono elementi ai quali, durante l'analisi, devono essere attribuiti un peso o una misura, sia per classificarli che per determinare una priorità di intervento. Ad esempio, è comune assegnare un "peso maggiore" a un rischio con alta frequenza di accadimento o che comporta gravi danni, mentre si assegna generalmente un "peso minore" a un rischio con minori probabilità di accadimento e che provoca pochi danni.
Il sistema di misura da usare nell'analisi è funzione degli obiettivi dell'analisi stessa: una misura di tipo quantitativo è normalmente più utile (ad esempio, consente la determinazione di un budget d'investimento più immediato), ma risulta più complessa da utilizzare, specie se non tutti gli elementi del problema sono noti.
Una misura di tipo qualitativo (basata ad esempio, su una scala di valori: basso, medio, alto, molto alto) è senz'altro di minore precisione, ma più applicabile nei casi pratici, ove non esistano elementi certi o dati statistici su cui basarsi.

Frequenza del processo di analisi

Per quanto riguarda la frequenza del processo analitico, esistono due approcci, "statico" e "dinamico".
L'approccio statico prevede una "fotografia" dello stato attuale, e richiede una revisione periodica (generalmente su base annuale) dell'analisi. Coinvolge l'intera amministrazione, richiedendo l'interazione di funzioni organizzative ben specifiche (*security manager, ICT manager*, comitato per la sicurezza).
L'approccio dinamico, viceversa, fornisce gli elementi per analizzare e gestire il rischio in modo continuativo e dinamico, basandosi su misure di tipo quantitativo.

Identificazione dei rischi a partire dai beni da proteggere

Obiettivo dell'analisi del rischio è, come detto, acquisire visibilità e consapevolezza sul livello d'esposizione al rischio dell'amministrazione, per poi costruire una lista preliminare dell'insieme delle possibili contromisure da attuare.
Uno dei percorsi più semplici consiste nel partire dall'identificazione dei beni (risorse) dell'amministrazione che necessitano protezione. La seguente tabella propone una possibile classificazione delle risorse, indicando per ogni tipologia di risorse le minacce maggiormente applicabili.

TIPOLOGIA DI BENI/RISORSE	RISCHI E MINACCE DA PRENDERE IN CONSIDERAZIONE
Hardware (terminali, postazioni di lavoro, stampanti, dischi, supporti di memorizzazione, linee di comunicazione, apparati di rete, …)	Malfunzionamenti dovuti a guasti, a sabotaggi, a eventi naturali come i terremoti, gli incendi e gli allagamenti, a furti e intercettazioni.
Software (di base o applicativo)	Presenza d'errori involontari commessi in fase di progettazione e/o implementazione che consentono a utenti non autorizzati di eseguire operazioni e programmi riservati, invece, a determinate categorie degli stessi. Presenza di codice malizioso volontariamente inserito in modo tale da poter svolgere operazioni non autorizzate sul sistema o per procurare danno allo stesso (virus, cavalli di Troia, bombe logiche, backdoor). Attacchi tipo denial of service (attacchi non distruttivi miranti alla saturazione delle capacità di risposta di un servizio che diventa, in tal modo, inutilizzabile).
Dati	Accessi non autorizzati, modifiche volute o accidentali.
Risorse umane	Minacce alla sicurezza e alla salute degli impiegati.
Documentazione (contratti, manuali)	Perdita di informazione per eventi naturali o errori umani.

Tabella 1

I beni e le risorse identificati vanno classificati in termini di sicurezza (integrità, riservatezza e disponibilità) necessaria, sia ai fini della corretta erogazione dei servizio, sia, più in generale, ai fini della sicurezza e della tutela del patrimonio pubblico. Questa classificazione è indispensabile per comprendere la funzione strategica dei beni stessi all'interno del sistema e poter, in seguito, valutare il livello d'esposizione al rischio.
Nella tabella seguente è riportato, a titolo indicativo, come potrebbero essere classificati i beni. Viene usata una misura di tipo qualitativo, che – come detto – è di utilizzo più semplice e immediato rispetto a una misura di tipo quantitativo.

	VALORE DEL BENE	LIVELLO DI SICUREZZA RICHIESTO
Bene 1	Alto	Molto Alto
Bene 2	Basso	Basso
Bene 3	Medio	Medio
…	Molto alto	Alto
Bene N	Basso	Medio

Tabella 2

Nella determinazione del valore dei beni dell'amministrazione, occorre considerare:

- il reddito del bene, ossia il reddito proveniente dall'utilizzo del bene;
- la perdita economica attesa dovuta alla perdita del bene, ossia la stima economica del danno subito dall'amministrazione e dal sistema pubblico nel suo complesso nel periodo in cui il bene non è disponibile.

Una volta determinati e classificati i beni da proteggere, il passo successivo è valutare la loro vulnerabilità alle varie minacce possibili. Come detto, è più agevole utilizzare una valutazione di tipo qualitativo. Il risultato di questa analisi potrebbe essere riportato in una tabella come la seguente, in cui in ogni cella è contenuto il grado di vulnerabilità di ciascun bene a fronte di ogni minaccia. Si noti che alcune minacce potrebbero non essere applicabili (N.A.) ad alcuni beni.

	Minaccia 1	Minaccia 2	Minaccia 3	…	Minaccia M
Bene 1	Bassa vulnerab.	Bassa vulnerab.	Bassa vulnerab.		N.A.
Bene 2	Bassa vulnerab.	Media vulnerab.	Media vulnerab.		Alta vulnerabilità
Bene 3	Media vulnerab.	Alta vulnerabilità	Media vulnerab.		Bassa vulnerab.
…	…				Bassa vulnerab.
Bene N	Alta vulnerabilità	N.A.	Bassa vulnerab.	Bassa vulnerab.	N.A.

Tabella 3

La valutazione delle vulnerabilità può avvenire tramite verifiche dirette, interviste e questionari[5].
L'utilizzo di strumenti come l'intervista o il questionario pongono, ai fini dell'efficacia, la problematica di presentare domande mirate e corrette alle persone giuste (in termini di ruoli ricoperti). Per determinare i corretti destinatari delle interviste, è utile partire dall'organigramma dell'amministrazione.
L'ultima classificazione utile è quella delle minacce, di cui deve essere stimata la probabilità (frequenza, di norma considerata su base annuale) di accadimento e il danno potenziale. Utilizzando ancora una misura di tipo qualitativo, è utile giungere a una classificazione come quella riportata nella tabella seguente.

	Frequenza di accadimento	Danno potenziale
Minaccia 1	Alta	Molto Alto
Minaccia 2	Bassa	Basso
Minaccia 3	Media	Medio
…	Molto alta	Alto
Minaccia N	Bassa	Medio

Tabella 4

Il valore dei beni, il livello di sicurezza richiesto, il livello delle vulnerabilità, la frequenza di accadimento e la stima del danno potenziale forniscono il livello complessivo del rischio cui è esposta l'amministrazione.
Esistono numerose statistiche sulle probabilità di accadimento delle minacce più tipiche. A titolo d'esempio, si riporta nella seguente figura un'elaborazione di una ricerca americana (*Contingency Planning Research*), che riporta le più probabili cause di disastro.
Una seconda statistica interessante è risultato di una rilevazione del Chartered Management Institute del 2004, in cui è stato chiesto a un campione di intervistati le cause delle emergenze (una o più) effettivamente verificatisi all'interno della loro organizzazione nel corso di un anno. Il risultato della rilevazione è riportato nella tabella 5.
Le statistiche citate si basano su informazioni storiche e risentono, ovviamente, degli ambiti geografici e territoriali di riferimento. Esse rappresentano soltanto un'indicazione a scopo esemplificativo. La frequenza di accadimento specifica della singola minaccia va quindi valutata volta per volta, come anche l'esposizione dell'amministrazione a ciascuna

[5] In alcune metodologie esistono schemi e modelli predefiniti che riportano il livello di vulnerabilità delle tipologie di beni più comuni, a seconda di alcune caratteristiche dei beni stessi. In questi casi la valutazione delle vulnerabilità viene effettuata sulla base di questi schemi, eventualmente adattandoli al contesto in esame.
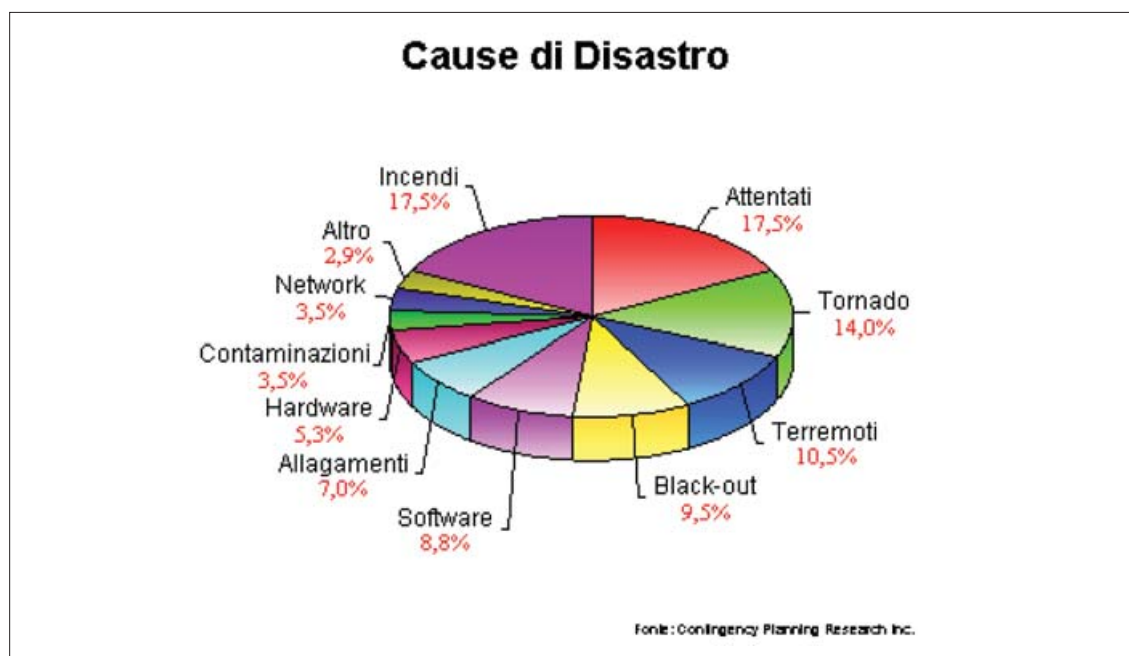
Figura 5

minaccia, eventualmente mediata attraverso l'efficacia degli strumenti di salvaguardia già in essere (controllo accessi, impianti di rilevazione e soppressione incendi, ridondanza degli apparati di alimentazione, ecc…).

Causa dell'emergenza	% delle risposte che hanno indicato questa causa
Perdita di capacità IT	25%
Perdita di telecomunicazioni	23%[6]
Perdita di personale	20%
Pubblicità negativa	16%
Perdita di competenze	14%
Interruzione della supply chain	12%
Inondazioni, cicloni	10%
Danno alla salute/sicurezza degli impiegati	8%
Danno alla reputazione dell'azienda	8%
Proteste di gruppi di pressione	7%
Perdita del sito	6%
Incendi	5%
Conflitti militari	5%
Problemi ambientali	4%
Danno alla salute dei clienti	4%
Attacchi terroristici	1%

Tabella 5

[6] Questa statistica, peraltro, conferma la scelta di concentrare la nostra indagine in particolare sugli aspetti legati all'IT e alle comunicazioni, che rappresentano le prime due cause effettive di disastro citate.

Una volta classificate le minacce, può essere utile rappresentarle graficamente come nella figura che segue. Sugli assi sono riportate la frequenza di accadimento e il danno potenziale. Un grafico del genere può permettere una prima grossolana indicazione di quali tipologie di contromisure debbano essere adottate per affrontare le varie minacce.
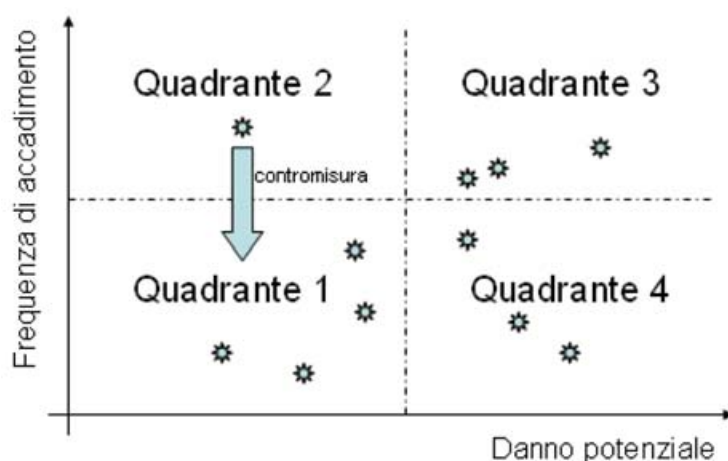
Figura 6

Generalmente, per bassi valori di frequenza e danno (quadrante 1), la minaccia si può ritenere "accettabile", e quindi l'adozione di contromisure può essere opzionale.
Viceversa, per valori elevati di frequenza e danno (quadrante 3), conviene intervenire radicalmente sulla minaccia (anche modificando in modo strutturale il contesto in cui viene realizzato il servizio minacciato).
Se la frequenza è elevata ma il danno potenziale è basso (quadrante 2), in genere si cerca di mitigare i danni attraverso opportune contromisure che rendano la minaccia meno probabile, in modo da riportare la minaccia nel primo quadrante del grafico.
Quando, infine, la frequenza è bassa ma il danno potenziale è alto (quadrante 4), può essere opportuno condividere il rischio con opportune soluzioni organizzative (centri comuni di backup, mutuo soccorso, ecc …) oppure trasferendo a terzi il rischio finanziario, ad esempio con contratti assicurativi (maggiori dettagli su queste soluzioni saranno dati al paragrafo 1.2).
In maniera più "rigorosa" rispetto alla tecnica "grafica" di cui sopra, l'analisi del rischio prosegue, tipicamente, con la determinazione del livello del rischio accettabile per l'amministrazione: in pratica, per ogni bene e per ogni minaccia, viene valutato il livello di rischio che l'amministrazione (o il sistema pubblico nel suo complesso) può accettare.
Tale livello è funzione di vari elementi quali:

- la missione istituzionale dell'amministrazione;
- i livelli di servizio previsti;
- la conformità alla normativa vigente;
- eventuali vincoli tecnologici e contrattuali;
- la disponibilità economica.

Il rischio accettabile viene confrontato con il rischio effettivo, determinando così il livello di rischio da abbattere, e di conseguenza le criticità e le priorità di intervento.

Il passo successivo consiste nel definire strategie di trasferimento o abbattimento del livello del rischio. Il trasferimento del rischio, in termini pratici, corrisponde alla sottoscrizione di una polizza assicurativa che copra alcuni aspetti del rischio (solitamente legati alla distruzione fisica dei beni). L'abbattimento del rischio, invece, consiste nell'adozione di una serie di salvaguardie (contromisure di natura fisica, logica o organizzativa) capaci di fornire protezione in termini di riduzione delle minacce e delle vulnerabilità e aiuto nelle azioni di recupero.
La determinazione delle possibili contromisure[7] viene effettuata su base tecnologica e organizzativa, ma anche economica, ossia tenendo presente il rapporto tra costi sostenuti e benefici. In altri termini, il costo dei meccanismi di protezione deve essere in linea con il valore dei beni soggetti a rischio[8].
Le contromisure sono caratterizzate da un costo di implementazione, di attuazione (costo di ripristino) e di manutenzione. Tuttavia, non è detto che la determinazione di tali caratteristiche avvenga nella fase di Risk Assessment.
Uno dei possibili prodotti di questa fase è riportato nella tabella seguente. Si tratta di una lista di interventi, classificati per priorità e correlati con le contromisure ipotizzabili per attuare gli interventi stessi.

	Priorità	Contromisura 1	…	Contromisura N
Intervento 1	Molto urgente	X		
Intervento 2	Urgente		X	X
…	…			
Intervento N	Bassa priorità	X		

Tabella 6

È anche possibile realizzare una tabella che indichi la "copertura" delle varie contromisure individuate, vale a dire su quali minacce le varie contromisure intervengono, e con quali effetti. Nella stessa tabella è utile riportare la valutazione dell'impatto che la contromisura ha sugli utenti del servizio (interni o esterni, da esplicitare se ha impatto diverso), il livello di accettazione ipotizzato da parte dei dipendenti dell' amministrazione coinvolti, e la complessità di implementazione della contromisura stessa.

	Minaccia 1	Minaccia 2	…	Minaccia N	Impatto su utenti	Livello di accettazione	Complessità
Contromisura 1	N.A.	Eliminazione		Riduzione	Alto	Basso	Alta
Contromisura 2	Eliminazione	Riduzione		Riduzione	Medio	Alto	Media
…					Basso	Alto	Media
Contromisura N	Eliminazione	Eliminazione		N.A.	Molto Alto	Basso	Alta

Tabella 7

A valle delle attività fin qui descritte, esiste la cosiddetta fase di "gestione del rischio", che si attua durante l'adozione e l'implementazione delle contromisure individuate, e si accompagna al monitoraggio dello stato della sicurezza.

[7] Si noti che questa attività è solo propedeutica alla effettiva scelta della soluzione di continuità da parte dell'amministrazione, che viene svolta in una fase successiva (vedi paragrafo 1.2).

[8] Per chiarire con un esempio di senso comune, nessuno comprerebbe una cassaforte da 1000 euro per proteggere un oggetto del valore di 100 euro.

1.1.2 BUSINESS IMPACT ANALYSIS (BIA)

Questa attività (il termine inglese è traducibile con "valutazione dell'impatto sull'operatività") ha lo scopo di determinare le conseguenze derivanti dal verificarsi di un evento critico e di valutare l'impatto di tale evento sull'operatività dell'amministrazione.
Prima di procedere, si sottolinea che anche questo paragrafo dev'essere inteso come momento di approfondimento di concetti già espressi in precedenza.
Lo svolgimento di una BIA segue in genere i tre passi descritti nel seguito.

Passo 1: individuazione dei servizi critici
Come detto in precedenza, nel settore pubblico, l'individuazione dei servizi critici può essere effettuata partendo dai procedimenti di competenza dell'amministrazione. Come ulteriore indicazione, si ritiene opportuno che l'analisi dei vari procedimenti non sia di particolare dettaglio. Tenendo presente la finalità dell'analisi (la continuità operativa), è consigliabile non scomporre un servizio, se esso viene supportato nella sua interezza da un unico sistema informatico.
Alcuni procedimenti, che non rientrano in modo chiaro ed evidente nelle primarie esigenze di continuità operativa dell'amministrazione, possono essere trascurati a priori (anche senza averli previamente analizzati).
Si deve tener conto che in molte amministrazioni la struttura dei procedimenti può essere soggetta a cambiamenti periodici anche significativi. Pertanto è opportuno prevedere un aggiornamento e raffinamento regolare della BIA: una periodicità ragionevole per l'aggiornamento è di 12-18 mesi.

Passo 2: identificazione delle "isole" a supporto dei servizi critici
È il passo più "tecnico". Deve essere svolto esaminando la documentazione tecnica e coinvolgendo (ad esempio tramite interviste) il personale operativo dell'amministrazione. Nell'individuazione delle risorse che supportano i servizi critici, si devono considerare gli aspetti infrastrutturali/logistici, organizzativi, tecnologici e applicativi, nonché le relative interconnessioni.
Relativamente alle risorse di tipo informatico, l'identificazione si può spingere sino all'analisi dell'architettura logica e fisica dei sistemi individuati.

Passo 3: analisi dell'impatto dell'indisponibilità prolungata
In questo passo si deve cercare di rispondere a due domande:

- per quanto tempo l'amministrazione può sopportare l'interruzione o il degrado prestazionale del servizio resosi indisponibile a fronte di un evento;
- in quale misura l'amministrazione può sopportare la perdita di dati associati al servizio in esame.

Normalmente, la BIA valuta l'impatto di un evento sull'operatività su base economica, valutando cioè la perdita economica causata dal verificarsi di un evento. Questo approccio, tuttavia, non è immediatamente applicabile al contesto della Pubblica Amministrazione. Nel settore pubblico, difatti, l'interruzione dei servizi erogati comporta danni non immediatamente "monetizzabili": le perdite (e dunque l'impatto) devono essere valutate tenendo conto dell'insieme dei seguenti aspetti:

- aspetti economici (mancata o ritardata riscossione di tributi, esborso di oneri aggiuntivi conseguenti il mancato pagamento a cittadini o imprese, ecc.);

- aspetti sociali (la non disponibilità di servizi sociali critici può generare problemi di ordine pubblico);
- aspetti reputazionali (perdita di credibilità da parte delle istituzioni);
- aspetti normativi (mancata o differita attuazione di norme di legge).

La particolarità del settore pubblico spiega perché a volte le amministrazioni debbano comunque adottare contromisure di prevenzione e contenimento del rischio anche quando il costo di tali contromisure sia superiore all'onere meramente economico dell'interruzione del servizio.
Oltre ai danni provocati dall'interruzione del servizio, per la valutazione di impatto occorre tenere conto dei danni legati a perdite di risorse di proprietà dell'amministrazione. Anche in questo caso, esiste una differenza significativa tra il settore pubblico e il settore privato: mentre nel settore privato le risorse di proprietà sono immediatamente valorizzabili per mezzo di un assessment, nel settore pubblico spesso la risorsa più importante e "di valore" gestita da un'amministrazione è il proprio patrimonio informativo. Si sottolinea che, in molti casi, le informazioni sono giuridicamente di proprietà dei cittadini, e l'amministrazione le gestisce per loro conto al fine di compiere la propria missione istituzionale.
Da ciò risulta che normalmente una BIA eseguita nel contesto di un'amministrazione pubblica assegna il massimo impatto agli eventi che minacciano l'integrità del patrimonio informativo dell'amministrazione.
Al termine dei passi descritti, in genere viene prodotto un documento finale di BIA. Un esempio di indice e di struttura è riportato nell'appendice A.
Nella BIA è possibile ritrovare numerosi concetti già espressi a proposito del *Risk Assessment* (ad esempio l'identificazione dei beni da proteggere). In effetti, le due attività (BIA e RA) presentano, nel contesto della continuità operativa, alcune aree di sovrapposizione. Ciò, unito al fatto che spesso il *Risk Assessment* è per le amministrazioni un'attività impegnativa in termini di tempo e risorse, suggerisce di concentrare gli sforzi sulla BIA, e di svolgere (eventualmente) il *Risk Assessment* a valle della BIA, a partire dai risultati di quest'ultima. Così facendo è possibile:

- evitare di ripetere il sottoinsieme di attività comuni (si cita ancora, come esempio, l'identificazione dei beni da proteggere);
- focalizzare il *Risk Assessment* sulle priorità e sugli obiettivi definiti nel corso della BIA, sempre con l'obiettivo di contenere i tempi e l'impiego di risorse per le attività di RA.

1.1.3 Recoverability assessment

Il *recoverability assessment* (traducibile in italiano con "verifica della capacità di mantenimento della continuità") è il terzo e ultimo passo previsto dall'analisi del contesto, e ha lo scopo di valutare l'effettiva capacità dell'amministrazione di soddisfare gli obiettivi di continuità prefissati mediante i processi, l'organizzazione e le risorse già in essere. In altre parole, durante questa fase si deve valutare la distanza (definita anche "gap") tra la situazione attuale e quella ottimale, cioè la situazione in cui tutte le esigenze di continuità sono soddisfatte.

In sintesi, gli obiettivi principali del *recoverability assessment* sono:

- descrivere l'effettiva capacità di mantenimento della continuità dei servizi critici dell'amministrazione;
- identificare gli elementi più critici (SpoF, single point of failure), ad esempio eventuali procedure obsolete, l'insufficienza o assenza di test di verifica periodica, l'incertezza dei ruoli e delle responsabilità che devono entrare in gioco prima, durante e dopo il verificarsi di un evento critico;
- indirizzare la successiva fase di definizione della soluzione di continuità.

I passi principali da seguire per il *recoverability assessment* sono:

- identificare cosa, dove, come e chi è coinvolto nelle operazioni di mantenimento della continuità;
- confrontare le attuali capacità di mantenimento del servizio con le capacità attese;
- organizzare e documentare le informazioni raccolte; ciò consentirà un processo di manutenzione della soluzione (*change management*) più snello.

L'importanza del *recoverability assessment* è dovuta al fatto che spesso le soluzioni di continuità operativa vengono realizzate in modo stratificato, in progetti successivi, dando ad esempio priorità a soluzioni che proteggono solo alcuni servizi particolarmente critici, e procrastinando l'adozione di soluzioni più generali. In questi casi, effettuare un corretto *recoverability assessment* garantisce la salvaguardia degli investimenti già effettuati.
A titolo di esempio, nel seguito vengono elencate le informazioni che possono essere raccolte durante un *recoverability assessment*:

1. descrizione del servizio da proteggere;
2. caratteristiche della relativa "isola";
3. caratteristiche dell'attuale backup dei dati (frequenza della copia completa, frequenza della copia incrementale, tipo di supporto che contiene le copie);
4. modalità di archiviazione delle copie (ad esempio salvataggio in luogo sicuro e distante dal centro di esercizio);
5. modalità e frequenza dei test;
6. stima del tempo per il ripristino a fronte di evento critico.

Nell'esaminare le attuali procedure di backup dei dati, si deve verificare se esse consentono il ripristino di dati *consistenti*. Difatti, le normali procedure di copia dei dati utilizzate a fini "applicativi", per ripristinare uno o più database con un contenuto precedente a un certo evento (copie complete/incrementali), non sono generalmente utilizzabili per ripristinare il servizio: a tale scopo si dovrà disporre di copie dei dati applicativi e di sistema *che abbiano relazioni logico/fisiche integre e congruenti tra loro.*
Per comprendere ulteriormente l'utilità di un *recoverability assessment*, si osservi il grafico seguente. Sull'asse delle ascisse è riportato il tempo occorrente, dall'istante dell'interruzione del servizio, per il suo ripristino. Sulle ordinate, viceversa, è riportato il costo della indisponibilità del servizio: esso è chiaramente funzione della durata temporale dell' indisponibilità.

Il *recoverability assessment* consente di capire dove si posiziona l'attuale situazione dell'amministrazione in termini di capacità di ripristino dei servizi, e di quantificare il gap da colmare per giungere a un livello di indisponibilità accettabile.
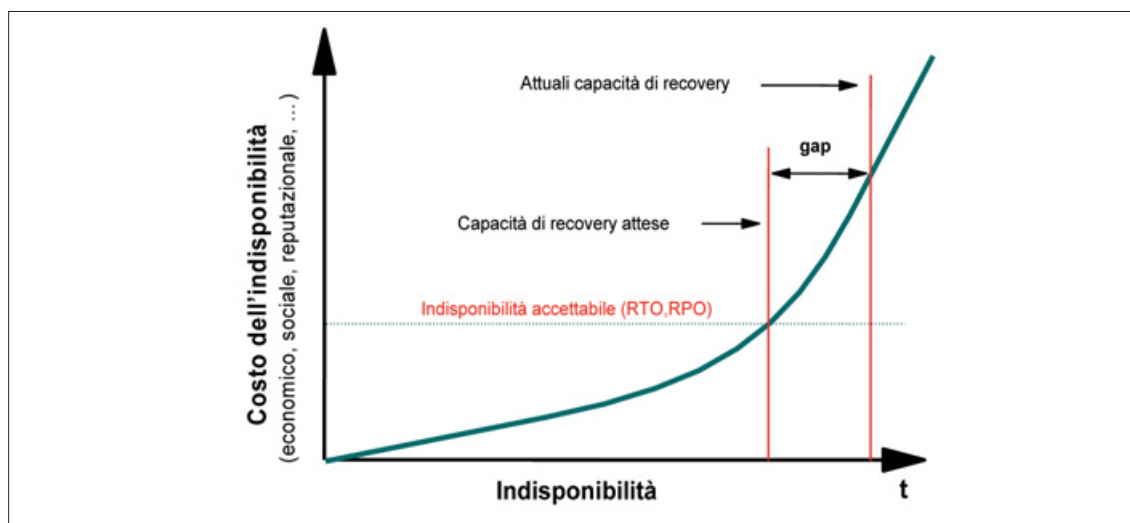
Figura 7

Le soluzioni di continuità operativa devono ridurre il costo dell'indisponibilità, sino a portarla a un valore ritenuto accettabile. Come si vedrà in dettaglio nel prossimo paragrafo, la realizzazione e il mantenimento di soluzioni di continuità comportano impegni economici la cui entità è funzione dei livelli di servizio scelti. Tipicamente, soluzioni che prevedono tempi di ripristino del servizio contenuti e una perdita dati tendente o uguale a zero sono molto più costose rispetto a quelle con livelli meno stringenti.
La figura seguente rappresenta in modo schematico il rapporto che lega il costo delle soluzioni con il costo dell'indisponibilità in funzione del tempo di ripristino.
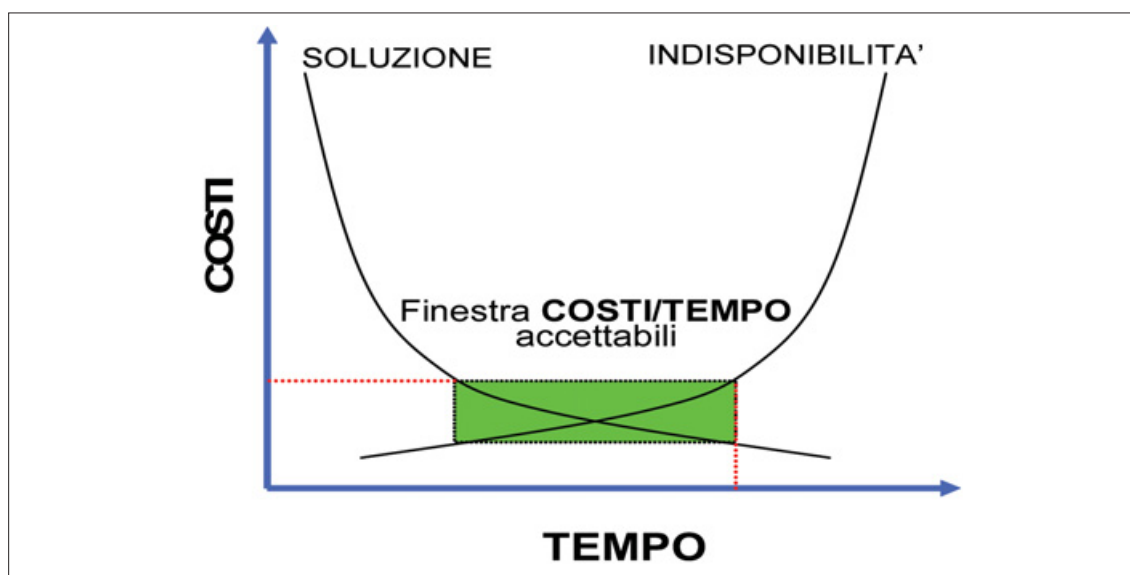
Figura 8

1.2 ESAME DELLE SOLUZIONI DI CONTINUITÀ POSSIBILI

Come detto in precedenza, è in genere possibile ipotizzare più soluzioni alternative che soddisfano le esigenze di continuità operativa riconosciute ed espresse come dettagliato nei paragrafi precedenti. Nel seguito verranno date alcune indicazioni, di ordine pratico, su come un'amministrazione può scegliere tra più soluzioni possibili.
Una soluzione di continuità è caratterizzata da numerosi fattori tra i quali:

- costo;
- semplicità realizzativa;
- garanzia di continuità offerta;
- livello di servizio in condizioni di emergenza.

Le soluzioni a basso costo, in genere, si basano quasi esclusivamente sulla pianificazione della risposta all'emergenza (cioè su una serie di regole e passi formali da svolgere in condizioni di emergenza), eventualmente accompagnata da interventi di natura organizzativa.
Il "livello base", che potremmo definire anche "soluzione a costo minimo", consiste nel predisporre un piano di continuità operativa che sarà eseguito al verificarsi di un incidente. Ciò corrisponde a definire un comitato di crisi e fissare le condizioni basilari (contatti, logistica, ecc.) per fare in modo che, in caso di emergenza, il comitato possa riunirsi e decidere gli interventi di ripristino (per un maggiore approfondimento sui piani di continuità operativa, si veda il paragrafo 1.4.3).
In genere queste soluzioni non consentono tempi di ripristino brevi. È comunque possibile ridurre tali tempi definendo alcune risposte "pre-determinate" che potranno essere intraprese in caso di emergenza: più risposte pre-determinate vengono previste dal piano (e dunque meno azioni vengono lasciate alle decisioni del momento), minore è il tempo che passerà tra il verificarsi dell'emergenza e il ripristino del servizio.
Le risposte che può essere opportuno predeterminare riguardano gli aspetti logistici, l'attivazione di una sede alternativa e dei relativi collegamenti telematici, la messa in linea delle applicazioni e la gestione dei sistemi, nonché il rientro alle condizioni ordinarie.
Ovviamente l'attività di pianificazione è fortemente condizionata dalla disponibilità di adeguate risorse per la gestione dell'emergenza (locali, hardware, software, linee di comunicazione…). Di solito, un piano articolato si accompagna a iniziative volte ad assicurare la disponibilità di tali risorse.
Tuttavia non di rado è possibile sviluppare un piano completo senza che sia necessario acquisire specifiche risorse dedicate al ripristino, utilizzando, ad esempio, strutture ridondanti già presenti nell'organizzazione, oppure ricorrendo ad accordi di mutuo soccorso (si veda a questo proposito il prossimo paragrafo).
Lo sviluppo del piano di continuità operativa[9] è dunque un'attività che può essere o meno correlata alla predisposizione di risorse per la gestione della situazione di crisi.

[9] In letteratura tale attività viene spesso referenziata con le seguenti espressioni in lingua inglese: contingency planning, business continuity planning, disaster recovery planning, business resumption planning, continuity planning.

La pianificazione dell'emergenza può essere condotta a vari livelli di dettaglio e considerando uno spettro più o meno ampio di evenienze. Qualunque sia l'articolazione del piano, per garantirne l'efficacia occorre che esso sia sottoposto a verifiche e prove periodiche. Anche il piano più semplice dovrà infatti essere periodicamente revisionato per controllare che sia rispondente all'effettivo contesto, ossia che riporti correttamente le informazioni relative alle figure professionali coinvolte e faccia riferimento a configurazioni, dispositivi o prodotti aggiornati.
Una pianificazione dettagliata delle attività di ripristino migliora sensibilmente la capacità di rispondere efficacemente all'emergenza ma, per contro, comporta costi non trascurabili per l'elaborazione e la verifica periodica del piano.

1.2.1 ACCORDI DI MUTUO SOCCORSO

La dizione "mutuo soccorso" deriva dalle omonime società sorte nella seconda metà dell'800, che offrivano appunto soccorso e aiuti a fronte di calamità e situazioni critiche. Tali soluzioni si caratterizzano – generalmente – per il basso costo e il basso livello di servizio. Sono basate su impegni di assistenza volontaria e non prevedono soluzioni tecniche complesse. Sono particolarmente adatte a fronteggiare situazioni di emergenza particolari, ove sia accettabile la possibilità di un periodo di discontinuità del servizio.
Le organizzazioni che stipulano un accordo di mutuo soccorso si offrono reciprocamente risorse, ospitalità e supporto logistico. Gli accordi possono essere modulati in relazione alle specifiche esigenze, da un semplice impegno d'aiuto sino a veri e propri patti che impegnano le organizzazioni a fornire livelli di assistenza predeterminati.
Generalmente, comunque, l'assistenza fornita all'organizzazione colpita dall'evento critico è "la migliore possibile" (cioè, semplicemente ciò che si può fare con le risorse a disposizione): la soluzione tecnica viene dettagliata nel momento in cui l'evento si manifesta.
Le soluzioni basate su accordi di mutuo soccorso sono tanto più efficaci quanto più sono simili le organizzazioni interessate. In particolare, le condizioni che favoriscono l'efficacia sono:

- comunanza di compiti;
- problematiche di continuità analoghe e non particolarmente stringenti;
- sistemi informativi con dimensioni e architetture simili;
- disponibilità di risorse per situazioni di emergenza (locali, CPU, spazio disco, ecc).

Gli accordi possono essere bilaterali o riguardare più di due organizzazioni. Nel secondo caso, ovviamente, cresce la complessità del piano d'emergenza. In particolare, gli accordi multilaterali devono comprendere un metodo formalizzato per la determinazione del destinatario della richiesta di soccorso: vale a dire, l'accordo deve specificare chiaramente a chi – tra le varie organizzazioni firmatarie – si deve chiedere aiuto nelle varie situazioni critiche; in alternativa, è opportuno che un ente terzo (ad esempio un organismo istituzionale) coordini le attività di soccorso in situazione di emergenza.
Esempio: un accordo di mutuo soccorso può prevedere che l'organizzazione soccorritrice renda disponibili locali attrezzati e apparati ausiliari (alimentazione, LAN, router, PC, ecc.) mentre l'organizzazione in emergenza provvede ad acquisire i server necessari per

ripristinare il servizio. Se quest'ultima dispone dei salvataggi dei dati e degli ambienti elaborativi, una volta che si è recuperato l'hardware è possibile ristabilire la configurazione e riattivare il servizio in tempi dell'ordine di 1-2 giorni. Nel caso di accordi tra più organizzazioni con sistemi analoghi, gli apparati necessari per il ripristino possono essere acquisiti anticipatamente con il contributo di tutti gli aderenti all'accordo e conservati in una sede opportuna, per poi essere trasportati all'occorrenza nel sito che ospita l'organizzazione in emergenza.
Per gli scopi della Pubblica Amministrazione, è opportuno approfondire due particolari tipologie di accordo di mutuo soccorso, cioè gli accordi tra organizzazioni indipendenti e gli accordi tra strutture di una stessa organizzazione.

Accordi tra organizzazioni indipendenti
Questo tipo di accordo si stipula normalmente quando un'organizzazione dispone di risorse logistiche ed elaborative sovrabbondanti rispetto alle esigenze ordinarie, per cui può ritenere conveniente individuare un partner che si trovi nella stessa condizione e abbia interesse a stipulare un patto di mutua assistenza per fronteggiare situazioni critiche.
Si noti che la condizione di "esubero di risorse", specie nel settore pubblico, si verifica di rado. Inoltre, spesso, la soluzione del mutuo soccorso trova ostacolo nelle esigenze di riservatezza verso organizzazioni estranee[10]. Per questo motivo gli accordi di mutuo soccorso tra organizzazioni indipendenti non sono molto frequenti e, di regola, non coinvolgono più di due organizzazioni.
L'accordo tipico tra organizzazioni indipendenti è scarsamente vincolante o non lo è affatto: ciascuna organizzazione assisterà l'altra solo a certe condizioni. Potrebbero perciò verificarsi circostanze particolari che impediscono il rispetto degli accordi (ad esempio una situazione di contemporanea emergenza nelle organizzazioni che hanno sottoscritto l'accordo).
Questo tipo di accordo può prevedere:

- un impegno generico di assistenza (in questo caso la modalità di soccorso viene determinata al momento di necessità);
- un salvataggio incrociato delle informazioni (ogni organizzazione, ad esempio, può conservare nei propri locali i dischi di backup dell'altra organizzazione) con periodicità fissata;
- un aiuto di tipo logistico (in caso di necessità vengono messi a disposizione locali attrezzati);
- la disponibilità di risorse elaborative e di comunicazione dedicate o condivise;
- la collaborazione del personale per le attività necessarie al ripristino dei servizi.

Gli accordi di mutuo soccorso meno vincolanti possono basarsi su un piano di continuità operativa elementare: in tal caso la cura delle attività di ripristino sarà demandata, al momento dell'emergenza, a un comitato di crisi cui è opportuno partecipino rappresentanti di entrambe le organizzazioni.

[10] Infatti in caso di necessità e durante le prove bisogna consentire all'organizzazione ospite di accedere alle proprie strutture informatiche e, benché sia possibile dedicarle ambienti elaborativi isolati, è difficile impedire che essa venga a conoscenza, almeno in parte, di informazioni (organizzazione, strutture, architettura, ecc.) che potrebbero avere un carattere riservato.

In caso di accordo più impegnativo, è opportuno che entrambe le organizzazioni, per rendere più efficaci le attività di ripristino, elaborino un piano di continuità operativa comune, ove siano determinate in anticipo le principali azioni che ciascuna parte compierà in caso di emergenza. In questo caso è consigliabile che le organizzazioni verifichino periodicamente l'efficacia del piano mediante prove congiunte.
Gli accordi tra organizzazioni indipendenti possono essere agevolati grazie al patrocinio di un ente terzo. Quest'ultimo può essere un organismo istituzionale che, per ruolo, promuove e favorisce accordi di mutuo soccorso tra organismi responsabili dell'erogazione di servizi ritenuti fondamentali[11]. In tal caso, l'ente terzo può essere parte attiva nella definizione dei piani d'emergenza e nel coordinamento delle attività di soccorso.

Accordi tra strutture di una stessa organizzazione

Sono gli accordi di mutua assistenza più frequenti, e vengono stipulati tra più strutture, facenti parte di una medesima organizzazione, che erogano servizi in modo autonomo (ad esempio filiali o sedi periferiche di uno stesso ente, dipartimenti di un'università).
In questo caso, lo schema di accordo potrà essere sviluppato da una struttura centrale, tenendo conto delle esigenze delle strutture che possono essere interessate. Ciascuna struttura potrà decidere se aderire o meno all'accordo; in caso di adesione, dovrà impegnarsi a soccorrere le strutture in condizioni di emergenza offrendo supporto logistico e rendendo disponibile parte delle proprie risorse elaborative[12].
L'accordo è quasi sempre di tipo multilaterale: la struttura centrale ha il compito di redigere un modello di piano di continuità operativa e uno schema di accordo che sia valido per tutta l'organizzazione. Ciascuna struttura aderente all'accordo dovrà personalizzare il piano di continuità operativa in funzione delle proprie specificità ed esigenze e dovrà predisporre le risorse occorrenti per eventuali attività di soccorso[13]. Nel caso in cui un'emergenza coinvolga più strutture, normalmente la struttura centrale svolge il ruolo di coordinamento dei soccorsi.

Vantaggi e svantaggi del mutuo soccorso

Come detto, il principale limite di questo tipo di soluzione è il suo approccio "volontaristico". A meno che non si basino su un contratto ben definito, accordi di questo tipo corrono il rischio di non essere onorati e l'organizzazione soccorritrice potrebbe non essere sempre disponibile a prestare assistenza quando occorre.
Chi sceglie una soluzione di mutuo soccorso, dunque, deve poter sopportare tempi di ripristino del servizio variabili anche in modo significativo. Se un'amministrazione ha esigenze di continuità più stringenti, questa soluzione deve essere scartata in favore di soluzioni che prevedano specifiche risorse (condivise o dedicate) deputate alle attività di ripristino.

---

[11] Questo ruolo potrebbe essere svolto dalla Protezione civile, da un Ministero o da un'amministrazione periferica.

[12] In alcune organizzazioni, l'adesione all'accordo di mutuo soccorso è obbligatoria per tutte le strutture. In questi casi però gli accordi sono quasi sempre di tipo vincolante, dunque le problematiche sono più simili a quelle dell'approccio basato su risorse condivise.

[13] A seconda della natura dell'organizzazione, la struttura centrale può avere un ruolo più o meno attivo nel definire le risorse logistiche, strumentali e di personale che ciascuna struttura deve predisporre. In alcuni casi l'accordo può prevedere che le strutture aderenti contribuiscano finanziariamente alla predisposizione di risorse comuni per l'emergenza. La struttura centrale può inoltre fungere da centro di backup centralizzato dei dati presenti nelle strutture che aderiscono all'accordo.

Può accadere inoltre che, nel tempo, le due organizzazioni che hanno stretto l'accordo facciano evolvere indipendentemente le proprie infrastrutture, fino a renderle incompatibili. Ancora, potrebbero avvenire dispute tra le due parti, inoltre insorgere questioni di sicurezza, di protezione della proprietà intellettuale e di informazioni confidenziali, tutte problematiche connesse alla natura di questo tipo di soluzione.
Nonostante questi limiti, gli accordi di mutuo soccorso possono rappresentare una valida soluzione in moltissimi casi: numerose amministrazioni, difatti, non hanno particolari esigenze di continuità operativa, ma devono semplicemente evitare la perdita del patrimonio informativo o l'interruzione prolungata dei servizi. In questi casi, gli accordi di mutua assistenza consentono di evitare queste evenienze con costi ridotti.
Esempi di amministrazioni che potrebbero trovare adeguata una soluzione di questo tipo sono scuole, musei, biblioteche, ospedali (limitatamente alle risorse dedicate ai sistemi gestionali), in generale amministrazioni medio-piccole.

1.2.2 La predisposizione di risorse per l'emergenza

Nell'ambito della predisposizione di risorse logistiche ed elaborative per l'emergenza, si possono adottare diverse soluzioni.
Le soluzioni più economiche sono basate sulla condivisione delle risorse tra più organizzazioni e possono sfruttare:

- centri di backup comuni;
- servizi di housing/hosting di società specializzate (cosiddetti "servizi di disaster recovery").

Costo ed efficacia di queste soluzioni dipendono dalla qualità e dalla quantità delle risorse "prenotate" e dal numero dei "clienti" che condividono tali risorse. Al crescere di questo numero, aumenta infatti il rischio che un evento critico possa coinvolgere più clienti che condividono la stessa risorsa di backup, e che tale contesa riduca l'efficacia del ripristino. Altri rischi sono legati alle caratteristiche del fornitore del servizio ed a fattori di tipo logistico e operativo.
Come indicazione pratica si propone, nel riquadro seguente, una serie di domande (una sorta di check-list) sulla base delle quali l'amministrazione può verificare l'adeguatezza fornitore.

Domande per la scelta del fornitore di servizi di disaster recovery

- Il fornitore è finanziariamente sano?
- Quanti sono i clienti con cui dovrei condividere le apparecchiature e/o i locali di cui ho bisogno?
- Quanti di questi si trovano entro un chilometro dalla mia sede (cioè chi presumibilmente sarà coinvolto nella mia stessa emergenza)?
- Chi tra questi clienti ha maggiore priorità?
- In caso di emergenza, se il sito di ripristino non è disponibile (magari perché occupato da un cliente con priorità maggiore della mia) quale soluzione alternativa mi viene prospettata?

(segue)

- Qual è la definizione di "emergenza" del fornitore (ovvero, in quali condizioni posso richiedere il servizio di ripristino)?
- In quanto tempo posso prendere possesso del sito?
- Quanto costa il canone annuale? E quali sono i costi di attivazione (cioè i costi da pagare al momento del ripristino)?
- Quali sono i costi per effettuare i test? Quanto tempo ho a disposizione per effettuare i test?
- Il fornitore è in grado di fornirmi oggi le apparecchiature e i servizi di telecomunicazione che mi necessitano? In caso contrario, come pensa di provvedere in futuro?
- Il fornitore ha sistemi UPS adeguati a sostenere l'intera installazione?
- Il fornitore manterrà aggiornate le apparecchiature in parallelo alle mie?
- Il fornitore supporterà vecchie apparecchiature fintanto che ne ho bisogno?
- Il fornitore è in grado di consegnare presso il mio sito piccole apparecchiature per evitare che io debba riallocare completamente i miei sistemi nel sito di ripristino? In tal caso, mi addebiterà costi aggiuntivi o il servizio è incluso nel canone annuale?
- L'utilizzo del sito di ripristino è accettabile per il mio personale? È facilmente raggiungibile da mezzi di trasporto pubblico? Sono disponibili aree di riposo, mensa, sale riunione per il personale? Esistono parcheggi adeguati?
- Il sito di ripristino è sicuro? I miei dati manterranno la confidenzialità necessaria?
- Il personale di supporto del fornitore è sufficientemente preparato?
- Il personale di supporto del fornitore mi aiuterà nelle fasi di ripristino?
- Il personale di supporto del fornitore mi aiuterà a effettuare i test?

Le soluzioni che offrono le maggiori garanzie di continuità, ma che risultano le più costose, sono quelle basate su risorse dedicate all'organizzazione. Tra queste soluzioni si può operare la seguente distinzione:

- soluzioni che prevedono un tempo significativo per creare le condizioni idonee ad operare in situazione di emergenza (ripristino a freddo);
- soluzioni che consentono di riattivare il servizio quasi immediatamente (ripristino a caldo).

Le prime prevedono che le risorse dedicate al ripristino si trovino in uno stato quiescente e possano divenire operative – in tempi che dipendono dalla specifica soluzione – tramite opportune operazioni pianificate in anticipo. Le seconde richiedono invece che le risorse dedicate al ripristino siano continuamente attive per poter subentrare "al volo" ai sistemi che dovessero trovarsi inaspettatamente in situazione di emergenza. La seconda tipologia richiede, ovviamente, maggiori costi, dovuti anche alla necessità di un continuo allineamento tra il sistema principale e quello di ripristino.

Nella letteratura tecnica, in realtà, si trova un'ulteriore suddivisione delle soluzioni che permettono il "ripristino a freddo". Si distingue tra:

- soluzioni che prevedono risorse già disponibili anche se in stato quiescente (stand-by) e che consentono un ripristino con tempi dell'ordine delle 24 ore (si parla talvolta di un "warm site");
- soluzioni che prevedono solo risorse di tipo logistico, che possono essere locali vuoti, prefabbricati o strutture mobili, dotati di elettricità, acqua e linee di comunicazione. La soluzione prevede che in tali locali vengano portate e installate, in caso di emergenza, le risorse necessarie al ripristino dell'operatività. La letteratura tecnica si riferisce a queste soluzioni anche con il termine "empty shell".

In generale, le soluzioni fondate sulla condivisione di risorse richiedono un elevato impegno per la gestione del piano, soprattutto per la necessità di pianificare adeguatamente le procedure di personalizzazione e inizializzazione dei sistemi di ripristino, e di effettuare frequenti prove e simulazioni per verificarne l'efficacia.
I sistemi dedicati possono invece essere già pre-configurati opportunamente. La gestione del piano è dunque più agevole e, in alcuni casi, può avvalersi di procedure per l'allineamento automatico delle configurazioni e dei dati tra il sistema principale e quello di ripristino. Inoltre, quando si adotta una soluzione in cui i sistemi di ripristino sono continuamente allineati al sistema principale (sistema di backup costantemente attivo), l'eventuale passaggio a tali sistemi non necessita di attività preparatorie e può avvenire in modo quasi completamente automatico: dunque la gestione della soluzione risulta ulteriormente semplificata.
La figura seguente mette a confronto le principali soluzioni tra quelle appena elencate, indicando in modo orientativo, per ciascuna soluzione, l'impegno economico necessario per la gestione della soluzione e quello per la predisposizione di risorse dedicate al ripristino.
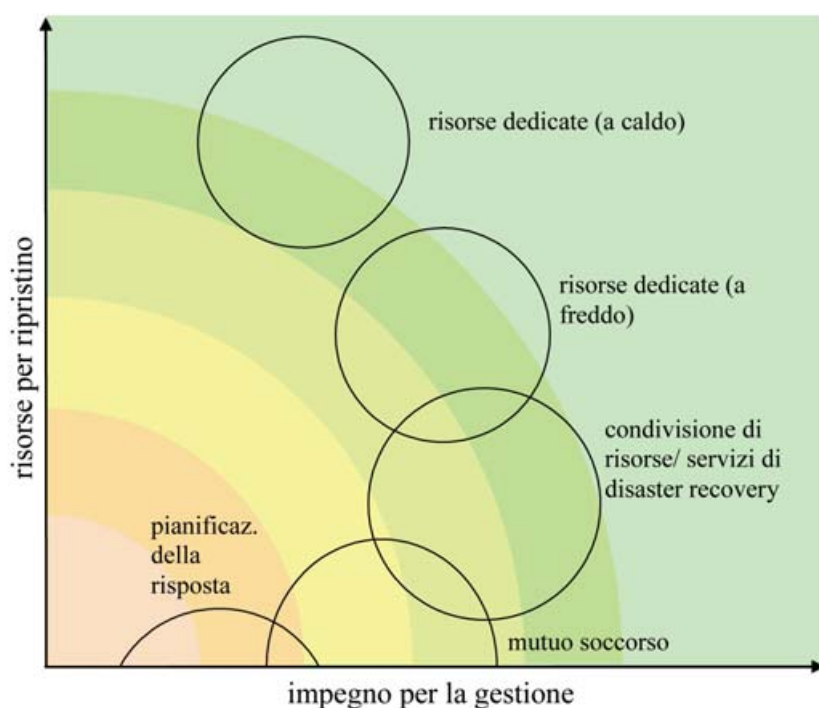
Figura 9

La figura illustra le differenze tra le possibili soluzioni in termini di gestione e di predisposizione delle risorse necessarie. Tuttavia, la classificazione che ne risulta non consente da sola una stima dei costi: occorre tenere conto di ulteriori fattori.
Ad esempio, nello stimare il costo di soluzioni basate su risorse dedicate, occorre tenere presente che, se da un lato è necessario approvvigionare consistenti risorse dedicate al ripristino, dall'altro tali risorse possono essere utilizzate anche in condizioni ordinarie, ad esempio per migliorare le prestazioni o la disponibilità dei servizi: dunque, nell'economia generale, tali scelte potrebbero risultare economicamente più convenienti rispetto ad approcci basati sulla condivisione di risorse.
È comunque ipotizzabile l'adozione di soluzioni miste. Ad esempio, una soluzione intermedia molto diffusa è quella che prevede che alcune risorse, come ad esempio gli elaboratori, siano totalmente dedicate ed altre, ad esempio i locali, siano condivise.
Restringendo l'esame alle soluzioni basate su risorse dedicate, la figura seguente confronta più nel dettaglio i costi e i tempi di ripristino delle soluzioni "a caldo" e delle soluzioni "a freddo". Come si vede in figura, si può stimare che le soluzioni "a caldo" costino da 3 a 5 volte di più delle soluzioni "a freddo".
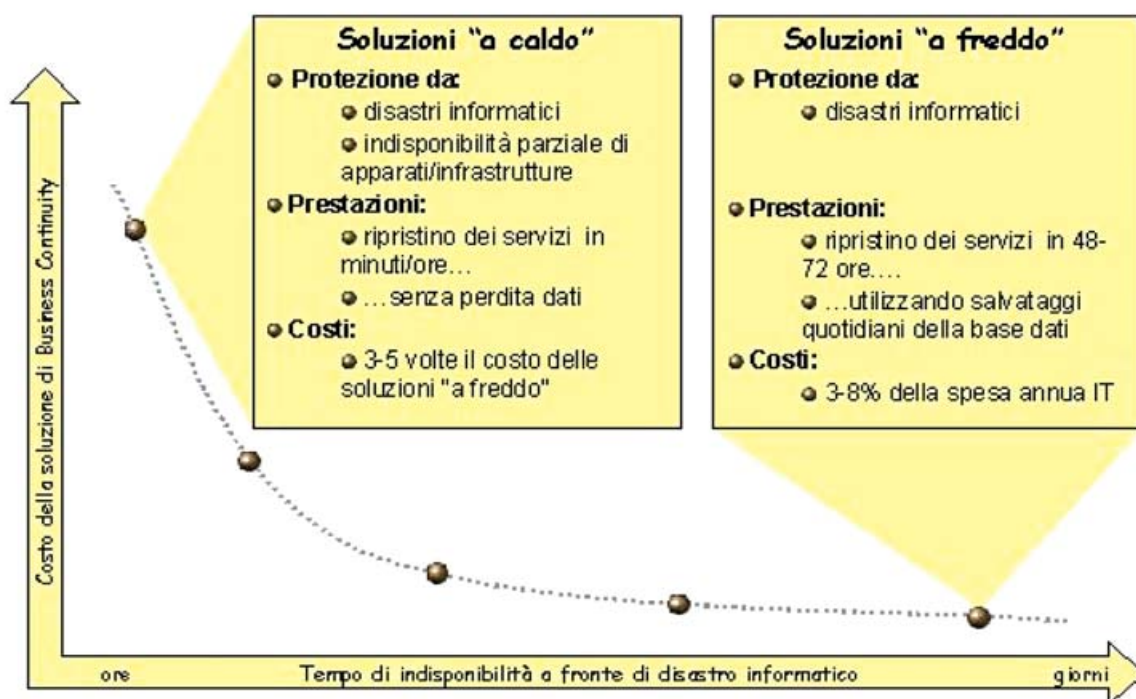
Figura 10

1.2.3 L'ADEGUAMENTO DELLE ARCHITETTURE

Un approccio complementare alla predisposizione di risorse per il recupero consiste nell'adottare soluzioni tecniche e organizzative che riducano fortemente l'impatto di possibili eventi critici.
Queste soluzioni tecniche e organizzative possono ricondursi alle seguenti tipologie:

- miglioramento delle procedure di backup;

- aumento della resilienza[14] del sistema;
- consolidamento.

Le attività di backup dei dati sono una prassi abituale nella gestione dei sistemi informativi, ma spesso sono progettate solo nell'ottica del recupero di informazioni a seguito di problemi ordinari. È possibile migliorare molto la risposta ai problemi di continuità operativa semplicemente riesaminando le procedure correnti di salvataggio dei dati nell'ottica del loro impiego per le attività di ripristino dopo un'emergenza. Gli interventi possono riguardare i luoghi e i locali di conservazione dei salvataggi (ad esempio, un intervento possibile è assicurarsi che i backup vengano conservati in luoghi diversi da quelli operativi), la loro duplicazione per incrementarne la disponibilità e l'inclusione nelle procedure di salvataggio di informazioni, anche non elettroniche, ritenute indispensabili per la riattivazione del servizio.
La seconda tipologia di soluzioni (aumento della resilienza) consiste nell'adottare architetture caratterizzate da un elevato tasso di resilienza ai guasti. Queste soluzioni si basano sulla ridondanza di apparati e processi e sulla capacità di operare, in condizioni di emergenza, anche se una parte delle risorse non è disponibile.
Una soluzione di questo tipo prevede risorse duplicate su siti diversi. In condizioni ordinarie entrambi i siti sono operativi e la ridondanza degli apparati viene sfruttata per garantire adeguati livelli di servizio. In condizioni di emergenza sarà invece operativo un solo sito che, seppure con prestazioni ridotte, offrirà tutti i servizi necessari. Se i due siti operano in modo speculare (tecniche di *mirroring*), è possibile fare in modo che il passaggio dalla condizione ordinaria a quella di emergenza avvenga in tempi ridottissimi, perfino in modo automatico.
Le soluzioni fin qui descritte prescindono dall'articolazione dei sistemi informatici responsabili dell'erogazione dei servizi. La scelta della soluzione è invece fortemente condizionata dalla struttura organizzativa, dalla logistica e dalle soluzioni tecniche adottate dall'amministrazione. In generale, all'aumentare della complessità architetturale – ossia della quantità ed eterogeneità dei sistemi elaborativi – aumenta anche la complessità delle soluzioni per il ripristino dell'operatività in condizioni di emergenza.
Nello scegliere la soluzione per la continuità operativa, può essere opportuno modificare la configurazione del sistema informatico con la finalità di rendere più economiche ed efficaci le attività di salvataggio e recupero. Quest'attività di razionalizzazione, o consolidamento[15], può essere parte dell'approccio alla gestione dell'emergenza, spesso in un'ottica di lungo termine.
Il consolidamento, che può riguardare diversi aspetti del sistema informatico (le basi dati, i sistemi, la rete, ecc.), deve essere comunque considerato come un'attività di ausilio alla realizzazione della soluzione di continuità operativa vera e propria.

1.2.4 Il trasferimento del rischio a terzi

Per completare il panorama delle possibili soluzioni, è utile menzionare soluzioni che potremmo definire di natura "contrattuale", in quanto prevedono che venga contrattualizzato, appunto, il coinvolgimento di un terzo nella gestione della continuità operativa.

[14] Con questo termine si indica la capacità di recuperare velocemente l'operatività a seguito di un problema. Spesso il termine resilienza è utilizzato come sinonimo di "fault tolerance" che indica la capacità di resistere ai guasti, oppure come proprietà di un'infrastrutture in grado di adattarsi ai picchi di richiesta per particolari servizi o applicazioni.

[15] Il termine "consolidamento" indica il procedimento di rendere più "solidi" i sistemi riguardo alla capacità di resistere a eventi critici. In genere, sotto questo aspetto, è preferibile ricorrere a sistemi di livello centrale che possono essere più facilmente gestiti da personale specializzato; a seguito di ciò il termine consolidamento è spesso usato con l'accezione di "accentramento".

Una classica soluzione di questo tipo è il trasferimento del rischio economico mediante forme assicurative.
Si noti, anzitutto, che difficilmente un'assicurazione può risarcire completamente le perdite dovute al verificarsi di un'emergenza, anche perché – come visto – esse sono difficilmente quantificabili. Può accadere che, alla stipula di un contratto assicurativo, non venga compreso correttamente il problema, e così venga sottoscritto un contratto che non offre una copertura adeguata (sottodimensionata, o sovradimensionata e perciò troppo onerosa).
A tal proposito, un recente studio effettuato dallo Health&Safety Executive[16] inglese mostra che perdite dovute a componenti non assicurati superano fino a 10 volte il costo dei premi assicurativi pagati.
Anche se il contratto viene stipulato in forma adeguata, in caso di emergenza ogni perdita da rimborsare va comunque dimostrata portando relativa traccia (fatture, perizie, ecc.), e tali documenti potrebbero non essere agevoli da produrre, o non rispecchiare correttamente i danni subiti (in genere al momento del risarcimento è necessaria una negoziazione). È perciò necessario pianificare attentamente cosa assicurare, l'assicurazione da scegliere, i periti indipendenti da nominare per la valutazione dei danni, ecc.
In ogni caso, la soluzione basata su copertura assicurativa non viene ritenuta idonea al contesto della Pubblica Amministrazione, sia perché non consente sempre il recupero delle perdite economiche (per i problemi appena detti), sia perché non garantisce la continuità dei servizi istituzionali.
Un approccio alternativo, più adatto al settore pubblico, consiste nel trasferire contrattualmente la responsabilità del mantenimento della continuità ai fornitori incaricati dell'erogazione dei servizi informatici. È opportuno prendere in considerazione tale possibilità soprattutto nel momento in cui si sceglie la strategia di acquisizione dei servizi ICT.
Ad esempio, nel caso di acquisizione dei servizi ICT in modalità ASP (Application Service Provider), l'amministrazione può demandare al fornitore la cura della continuità dei servizi informatici, semplificando in modo considerevole il piano di continuità operativa, che, in tal caso, dovrebbe curare i soli aspetti logistici e organizzativi.
Analogamente, nel caso di outsourcing, molte delle problematiche di continuità operativa possono essere demandate al fornitore.
In generale, anche nei casi in cui l'amministrazione sceglie di sviluppare "in proprio" la soluzione di continuità, è opportuno tenere presente che molti processi che concorrono a garantire il servizio sono di norma affidati a soggetti terzi (ad esempio i servizi di comunicazione). Garantire la continuità operativa significa anche assicurare la disponibilità di tali servizi.
In generale questo obiettivo può essere raggiunto con due approcci diversi:

- prevedendo soluzioni alternative nel caso di indisponibilità prolungata del servizio esterno;
- richiedendo che il fornitore del servizio abbia una propria soluzione di continuità.

Il secondo approccio richiede che la soluzione di continuità sia prevista contrattualmente, cioè che il contratto definisca le caratteristiche e i parametri di qualità della soluzione che il fornitore deve adottare[17].

[16] http://www.hse.gov.uk/betterbusiness/hsebooklet.pdf.

[17] Le consuete clausole contrattuali relative ai livelli di servizio non sono sufficienti a garantire la continuità operativa, per il fatto che nel caso di inosservanza dei parametri contrattuali il fornitore è tenuto al più al pagamento delle penali. Ai fini della continuità operativa è invece necessario che il contratto preveda anche una obbligazione di mezzi, definendo gli strumenti che il fornitore dovrà impiegare per garantire la continuità del servizio anche a seguito di eventi critici.

Un'altra possibilità di coinvolgimento di soggetti terzi nella strategia di continuità operativa consiste nella stipulazione di accordi con i fornitori per la consegna, in tempi predeterminati, dei beni utili al ripristino dell'operatività. Questi accordi, di norma, riguardano sistemi hardware e software da acquisire nel caso di attivazione del piano di continuità operativa e possono essere parte del contratto di fornitura delle macchine di esercizio.
In particolare, si cita la cosiddetta "fornitura veloce" (definita a volte in letteratura col termine "quick ship"), meglio descritta nel seguito.

Fornitura veloce
Si tratta di un accordo stipulato con un fornitore, in base al quale questi s'impegna a consegnare in tempi molto rapidi, presso la sede indicata, apparecchiature, impianti o altro, in sostituzione di risorse danneggiate dal verificarsi di un'emergenza. Questi accordi prevedono, in genere, un canone fisso per ottenere la priorità nella ricerca dei ricambi, più un premio da versare quando si richiede effettivamente la spedizione del pezzo in sostituzione.
Come esempio pratico si può considerare il caso di un sistema di stampa utilizzato per la produzione di cedolini o altra certificazione da fornire all'utenza. Il sistema di stampa potrebbe già essere sotto contratto di manutenzione, ma tale contratto potrebbe stabilire livelli di servizio che l'amministrazione giudica incompatibili con le proprie esigenze di continuità (es. risoluzione dei problemi entro 48 ore dalla chiamata). In questo caso l'amministrazione potrebbe ricorrere alla "fornitura veloce" per disporre comunque di un sistema di stampa funzionante entro un tempo fissato. Il contratto di fornitura veloce potrebbe rimpiazzare completamente il contratto di manutenzione, oppure potrebbe inglobarlo, nel senso che il fornitore s'impegna a fornire in comodato d'uso l'apparecchiatura alternativa per tutto il tempo necessario a ripristinare l'operatività dell'apparecchiatura danneggiata.
Orientativamente, queste soluzioni si possono posizionare, nel diagramma dei costi delle soluzioni, nell'area indicata per gli accordi di mutuo soccorso.
Come variante della fornitura veloce, esiste il cosiddetto "servizio di immagazzinamento". In questo caso le risorse alternative sono di proprietà dell'amministrazione, e al fornitore viene dato carico di conservarle in un sito sicuro, per poi prelevarle e consegnarle in tempi rapidi (fissati contrattualmente) all'amministrazione in caso di indisponibilità delle risorse principali. Oltre alle risorse alternative, al fornitore potrebbe essere affidato il compito di conservare anche dati di backup o particolari documenti da proteggere.
Per tornare all'esempio precedente, l'amministrazione potrebbe decidere di acquistare un secondo sistema di stampa: in questo caso il fornitore si impegna semplicemente a conservarlo in un suo magazzino e a trasportarlo presso i locali dell'amministrazione quando questa lo richiede. Ovviamente il costo di questo servizio è più basso rispetto al servizio di fornitura veloce, ma presuppone un investimento iniziale più alto da parte dell'amministrazione.

1.2.5 Altri servizi di ripristino

Per completezza si citano alcuni servizi disponibili sul mercato, che possono essere di interesse per le pubbliche amministrazioni, anche se non tutti sono necessariamente indirizzati alla risoluzione di problemi di continuità operativa. Si tratta di:

- servizi speciali di telefonia, quali offerta di percorsi alternativi garantiti di reindirizzamento di comunicazioni telefoniche e dati;

- disponibilità di personale temporaneo per far fronte a emergenze che riguardano la forza lavoro;
- servizi di stoccaggio e archiviazione sicura di materiale e documentazione;
- affitto di attrezzature e materiale da ufficio;
- forniture di apparecchiature di seconda mano.

1.2.6 CLASSIFICAZIONE DELLE AMMINISTRAZIONI

Per scegliere la soluzione di continuità operativa più adatta alle esigenze di una amministrazione, è utile riferirsi a casistiche predefinite: si ritiene infatti che le soluzioni ottimali dipendano in modo prevalente dalla natura dei compiti e dalla struttura delle varie amministrazioni.
Nel seguito viene presentata una classificazione delle amministrazioni finalizzata a delineare situazioni caratterizzate da problematiche comuni di continuità operativa e a individuare soluzioni idonee per ciascuna categoria[18].
La classificazione è basata sui parametri che definiscono le esigenze di continuità operativa delle amministrazioni, ad esempio il tempo massimo di interruzione tollerabile (RTO). In realtà tale parametro – come detto – non dipende dal tipo di amministrazione ma dalla natura dei singoli procedimenti amministrativi e può variare, nell'ambito di una stessa amministrazione, in funzione dell'ufficio o del periodo dell'anno. Per semplificare la trattazione, si è supposto che, all'aumentare della complessità dell'amministrazione, aumenti anche la probabilità che vi siano attività istituzionali che non possono tollerare tempi di interruzione del servizio significativi e, in base a tale considerazione, si è ipotizzato un intervallo plausibile di valori del parametro RTO[19].

Amministrazioni di classe A
Si tratta di amministrazioni medio-piccole dislocate in un'unica sede. Le attività svolte non sono in genere particolarmente critiche ai fini della continuità operativa e può essere tollerata una interruzione del servizio per una durata massima variabile tra giorni e settimane.
Il sistema informatico è costituito da PC e server connessi in LAN. La presenza di personale tecnico è limitata e le attività di gestione degli apparati e dei programmi sono affidate a soggetti terzi. I servizi informatici vengono erogati presso gli stessi uffici.
Esempi di tali amministrazioni sono: comuni di dimensioni piccole o medie, province, amministrazioni centrali di piccole dimensioni.

Amministrazioni di classe B
Fanno parte di questa categoria amministrazioni medio-grandi dislocate su più sedi in una stessa località geografica (ad esempio nello stesso comune). Dal punto di vista della continuità operativa, la maggior parte delle attività che vi si svolgono presentano un livello di cri-

[18] Sono escluse da questa classificazione – e dunque dall'intero studio – le amministrazioni la cui continuità operativa è un elemento essenziale per la sicurezza dello Stato e dunque non può essere trattata in documenti pubblici (servizi di intelligence, centri di comando, caserme, ecc.).

[19] Si ricorda che nel caso le amministrazioni trattino dati sensibili o giudiziari, il Codice in materia di protezione dei dati personali impone di fatto il limite di 7 giorni (punto 23 dell'allegato B: *sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni*).

ticità medio (interruzione massima dell'ordine di giorni-settimane), ma possono esservi specifici servizi per i quali non è tollerabile un periodo di interruzione superiore a un giorno.
Il sistema informatico è costituito da più LAN tra loro interconnesse. Ogni ufficio ha una propria LAN e diversi terminali, mentre i server sono allocati in una specifica sede (generalmente la sede centrale). Presso tale sede è presente personale tecnico in grado di effettuare le operazioni di backup/restore e di gestione ordinaria. I servizi sono erogati presso gli uffici tramite collegamenti remoti ai sistemi server, oppure attraverso Internet.
Esempi di tali amministrazioni sono: comuni di dimensioni medie o grandi, regioni, amministrazioni centrali di dimensioni medie.

Amministrazioni di classe C
Rientrano in questa categoria amministrazioni complesse dislocate su più sedi in una stessa località geografica (ad esempio nello stesso comune). Rispetto alle amministrazioni della classe precedente cambia, principalmente, la complessità dei compiti e il numero di utenti interni ed esterni.
Dal punto di vista della continuità operativa, le attività che vi si svolgono presentano un livello di criticità significativo, in quanto molti dei servizi erogati non possono essere interrotti per periodi superiori a 1-3 giorni.
Il sistema informatico è costituito da più LAN tra loro interconnesse, alcune delle quali dotate di propri sistemi server. Presso una specifica sede (generalmente la sede centrale) sono presenti strutture dedicate a ospitare i sistemi elaborativi (sale server o CED). Presso tali strutture è spesso presente un sistema di classe mainframe. L'organigramma comprende un'unità organizzativa avente il compito di curare gli aspetti informatici. I servizi sono erogati presso gli uffici tramite i server locali o mediante collegamenti remoti ai sistemi server, oppure tramite Internet.
Esempi di tali amministrazioni sono: comuni metropolitani, regioni, ASL, amministrazioni centrali.

Amministrazioni di classe D
Le amministrazioni appartenenti a questa categoria hanno strutture complesse e articolate dislocate su più sedi nel territorio nazionale. Di norma offrono uno spettro ampio dei servizi e per alcuni di essi la disponibilità è una caratteristica essenziale. Il tempo massimo di interruzione che può essere tollerato varia a seconda della tipologia di servizi ed è compreso tra ore e giorni.
Il sistema informatico ha un'architettura complessa che comprende server di diverso livello, periferici e centrali. A seguito della stratificazione degli interventi di informatizzazione, le configurazioni sono di solito eterogenee. A livello centrale è spesso attivo un sistema di tipo mainframe.
L'organigramma comprende più unità organizzative aventi il compito di curare gli aspetti informatici. Talvolta le sedi periferiche sono dotate di propri uffici preposti alla gestione dei sistemi. I servizi sono erogati in vario modo, talora utilizzando i sistemi locali, talvolta ricorrendo alle risorse del sistema centrale. Tutte le postazioni di lavoro sono collegate mediante le rete interna (intranet). Alcuni servizi verso il pubblico o verso il settore finanziario e industriale sono erogati tramite Internet.
Fanno parte di questa classe le grandi amministrazioni centrali e gli enti previdenziali.

Tabella riassuntiva

La tabella seguente riepiloga la classificazione esposta.

CARATTERISTICHE	TIPOLOGIA DI AMMINISTRAZIONE			
	CLASSE A	CLASSE B	CLASSE C	CLASSE D
Numero di sedi	1	2-6	2-12	> 3
Numero di sedi con server	1	1	≥ 1	> 1
Sedi in diverse aree geografiche	no	no	no	si
Tipo di server[20]	PC/mini	mini	mini/MF	mini/MF
Strutture attrezzate per server[21]	no	no	si	si
Personale tecnico dell'amministr.	no	si	si	si
Ufficio informatico	no	no	si	si
Periodo di interruzione tollerabile	giorni settim.	giorni-settim.	giorni	ore-giorni

Tabella 8

1.2.7 CLASSIFICAZIONE DELLE SOLUZIONI

Per scegliere la soluzione di continuità più adeguata, l'amministrazione deve individuare il migliore equilibrio tra le seguenti esigenze:

- il contenimento dei costi;
- la capacità di ripristino dei servizi essenziali in tempi accettabili;
- l'efficacia della soluzione al verificarsi delle possibili emergenze;
- la qualità e la sicurezza dei servizi nella fase di emergenza;
- il limitato impatto della della soluzione sulle prestazioni del sistema in esercizio[22].

Per quanto riguarda i costi, è utile distinguere tra quelli dovuti alla predisposizione della soluzione (costi "una tantum" per la stesura del piano e per le infrastrutture) e quelli che occorre sostenere per mantenere la soluzione efficace nel tempo (costi "ricorrenti" di gestione della soluzione). Questi ultimi comprendono i costi di personale per la gestione del piano, le prove periodiche, i costi per la trasmissione dei dati verso il centro di ripristino, ecc.
È opportuno inoltre considerare, oltre ai costi menzionati, anche i costi che devono essere sostenuti:

- nel momento in cui si attiva il piano d'emergenza;
- nel periodo di emergenza;
- nella fase di rientro.

[20] Le tipologie prese in considerazione sono le seguenti: (PC) personal computer con sistema operativo Microsoft o Linux (PC); (mini) sistema con processore Intel o AMD con caratteristiche prestazionali e di affidabilità tipiche di un server e sistema operativo Microsoft o Unix; (MF) sistema legacy con sistema operativo proprietario o Unix.

[21] Per strutture attrezzate si intende l'impiego, presso almeno una sede, di locali dedicati alle macchine con impianti di condizionamento, di continuità e sistemi anti-incendio ed anti-intrusione.

[22] Ad esempio, una soluzione di tipo sincrono può introdurre ritardi nei tempi di risposta del sistema.

Molti di questi costi (maggiori costi di personale, trasferte, trasporti, acquisto di beni, servizi di comunicazione, eventuali tariffe per i servizi che sono attivati nel momento della dichiarazione dell'emergenza, ecc.) prescindono dalla durata del periodo di emergenza, e devono essere sostenuti anche nel caso l'evento negativo si ridimensioni prima di aver avviato i servizi di continuità operativa.
La tabella seguente schematizza la composizione dei costi.

	VOCI DI COSTO	TIPO
Predisposizione della soluzione	Piano di continuità operativa, locali, apparati, prodotti sw, linee/servizi di comunicazione	Unatantum/ricorrente[23]
Gestione della soluzione	Prove periodiche, adeguamento del piano adeguamento delle configurazioni, canoni per servizi di comunicazione …	Ricorrente
Avvio piano di continuità operativa/rientro alla normalità	Maggiori prestazioni del personale trasporti, acquisto ulteriori beni servizi per l'emergenza …	Per evento

Tabella 9

Come ulteriore fattore di scelta della soluzione si consiglia di considerare anche la versatilità della soluzione, intesa come la capacità di risolvere problemi di discontinuità del servizio in un ampio spettro di circostanze[24].
La tabella che segue riassume, in colonna, le principali caratteristiche delle soluzioni individuate nei paragrafi precedenti. Le caratteristiche sono le seguenti:

- il costo (in termini qualitativi) della soluzione, scomposto nelle sue principali componenti secondo quanto riportato nella tabella precedente;
- il tempo di ripristino del servizio che la soluzione consente (come ordine di grandezza);
- la versatilità della soluzione;
- la qualità del servizio che può essere garantita in condizioni di emergenza (in termini di tempo di risposta, disponibilità, ecc.) e le garanzie di sicurezza[25].

In questa classificazione delle soluzioni si sono trascurati alcuni fattori. Ad esempio, il parametro RPO, in questa prima analisi, non è stato riportato, in quanto si ritiene che incida meno degli altri fattori per la scelta della soluzione. Generalmente, il RPO è invece un elemento importante per definire la periodicità dei salvataggi dei dati, a prescindere dalla tipologia di soluzione.

[23] I costi di infrastruttura possono essere una tantum o ricorrenti a seconda che si scelga di acquistare o noleggiare i beni.

[24] I sistemi di continuità operativa sono stati inizialmente introdotti per fronteggiare eventi di tipo calamitoso (inondazioni, terremoti, ecc.), l'esperienza ha però mostrato che un fermo prolungato può essere cagionato dagli eventi più disparati, com'è stato detto.

[25] Di solito in condizione di emergenza si accetta che i livelli di servizio e di sicurezza siano inferiori a quelli che è possibile garantire in situazione ordinaria, tuttavia per molte applicazioni non è accettabile scendere sotto una determinata soglia, per cui questo fattore può condizionare la scelta della soluzione.

TIPOLOGIA DI SOLUZIONE	COSTO			TEMPO DI RIPRISTINO DEL SERVIZIO	VERSATILITÀ	QUALITÀ E SICUREZZA SERVIZI IN EMERGENZA
	PREDISPOS. SOLUZIONE	GESTIONE SOLUZIONE	AVVIO/ RIENTRO			
Pianificazione e risposta	Basso	Basso	N.A.[26]	Settimane/ mesi	Bassa	Bassa
Mutuo soccorso	Basso	Medio	Alto	Settimane	Bassa	Bassa
Condivisione di risorse	Medio	Medio/alto	Alto	Giorni/ settimane	Bassa	Media
Risorse dedicate (a freddo)	Alto	Medio	Medio	Ore/giorni	Media	Medio/alta
Risorse dedicate (a caldo)	Alto	Medio/ basso	Basso	Ore	Alta	Alta
Consolidamento/ aumento della resilienza[27]	N.A.[28]	Medio	Molto basso	Minuti	Medio/alta	Medio/alta
Trasferimento rischio a terzi (ASP, outsourcing, immagazzinamento)	Alto	Medio/alto	Basso	In funzione del contratto	Alta	Bassa
Fornitura veloce	Basso	Medio/ basso	Alto	Ore/giorni	Medio/ bassa	Bassa

Tabella 10

Si noti che a volte la scelta della soluzione può essere condizionata da fattori contingenti che poco hanno a che fare con le caratteristiche del servizio. Ad esempio potrebbe essere importante:

- la posizione geografica del sito principale;
- l'architettura del sistema informativo (centralizzata, decentralizzata, ecc.) e la sua adattabilità alle esigenze di continuità;
- la possibilità di uso di opportuni locali per il ripristino;
- la disponibilità di centri servizio attrezzati;
- i servizi di comunicazione disponibili e i loro costi;
- le relazioni o i protocolli d'intesa esistenti tra amministrazioni diverse.

[26] Il costo da affrontare nei casi di emergenza dipende da diversi fattori, tra cui la complessità del sistema elaborativo da ripristinare (eventualmente acquisendo gli apparati all'occorrenza). In genere si tratta di un costo elevato.

[27] Le soluzioni "Risorse dedicate a caldo" e "Consolidamento/aumento della resilienza" sono simili sotto l'aspetto tecnologico, la prima però si basa su un sistema dedicato o su servizi di disaster recovery con risorse dedicate, la seconda non introduce elementi aggiuntivi ma risolve i problemi di continuità operativa con soluzioni architetturali. Il secondo approccio comporta minori costi di gestione ma può essere meno efficace in talune circostanze (ad esempio problemi che coinvolgono più sedi) e può comportare un degrado delle prestazioni in condizioni di emergenza.

[28] Non vi sono costi per infrastrutture dedicate, la soluzione però richiede la revisione dell'architettura con costi che dipendono fortemente dal contesto, ma sono generalmente elevati.

1.2.8 MATRICE TIPO-AMMINISTRAZIONE/SOLUZIONI

Di regola non è possibile individuare la soluzione di continuità più opportuna senza una preventiva analisi dei possibili eventi negativi e delle implicazioni che tali eventi comportano (si veda il paragrafo sulla *Business Impact Analysis*). Ciò premesso, nel seguito viene illustrata, per ciascuna categoria di amministrazioni, una rosa di possibili scelte, con riferimento alle soluzioni appena illustrate.

Soluzioni per amministrazioni di classe A

Nel caso di piccole amministrazioni, generalmente il fattore costo è preponderante nella scelta della soluzione. Inoltre raramente sono necessari tempi ridotti per il ripristino del servizio. Sono dunque idonei gli approcci che permettono di affrontare eventi calamitosi garantendo gli adempimenti essenziali anche senza elevati livelli di servizio.
In tal senso sono particolarmente indicati gli accordi di mutuo soccorso o forme associative che consentono di condividere le risorse per l'emergenza. È inoltre possibile ricorrere a servizi di *disaster recovery* basati su risorse condivise tra più amministrazioni.
Anche la predisposizione del piano di continuità operativa può essere semplificata ricorrendo a modelli predefiniti relativi ad amministrazioni con problematiche analoghe (ad esempio comuni omogenei).
Una possibilità che è opportuno valutare è il ricorso a un modello di erogazione dei servizi informatici che demandi al fornitore tutti gli aspetti tecnici (ad esempio in modalità ASP o ricorrendo a centri servizi). In questo caso l'amministrazione potrà sviluppare un piano di continuità operativa che si preoccupi essenzialmente degli aspetti logistici e organizzativi, mentre sarà cura del fornitore adottare un proprio sistema di continuità operativa che garantisca i servizi informatici.
In alternativa, nel piano di continuità operativa, occorrerà prevedere una modalità per acquisire l'hardware e il software necessario in condizioni di emergenza. Poiché normalmente si tratta di apparati di costo non elevato e di tipologia standard, questo problema può anche essere risolto acquisendo all'occorrenza gli apparati, eventualmente previo accordo con i fornitori per garantire i tempi di consegna (vedi le forniture veloci).
Tra le attività a carico dell'amministrazione, si evidenzia l'opportunità di rivedere le procedure di salvataggio dei dati nell'ottica di un loro utilizzo per la continuità operativa.

Soluzioni per amministrazioni di classe B

Le amministrazioni di questa classe hanno una configurazione semplice per quanto concerne i sistemi elaborativi, ma una struttura abbastanza complessa relativamente agli uffici e ai punti di accesso ai servizi.
Per tale motivo, le soluzioni per il ripristino dei soli servizi informatici (*disaster recovery*) possono ricondursi a quelle delle amministrazioni di classe A (mutuo soccorso, condivisione di risorse), salvo i casi in cui la natura degli adempimenti amministrativi imponga tempi più bassi per il ripristino dei servizi. In quest'ultimo caso si può ricorrere a soluzioni basate su risorse dedicate o a soluzioni miste, eventualmente utilizzando servizi di *disaster recovery*[29].

[29] Un esempio di soluzione di quest'ultimo tipo è quella che prevede un ambiente elaborativo dedicato (*Virtual Machine*) su un elaboratore condiviso.

Sempre nell'ottica di predisporre soluzioni con basso valore del RTO, si può valutare l'opportunità di duplicare parte delle risorse elaborative presso una seconda sede dell'amministrazione, sfruttando sistemi di allineamento automatico dei dati. Si ricordi però che tale soluzione introduce una complessità tecnologica che potrebbe risultare problematica in assenza di personale con adeguata preparazione tecnica.
Un'alternativa a queste soluzioni consiste nella completa esternalizzazione dei servizi informatici a un centro servizi specializzato e dotato di opportuni sistemi di continuità operativa.
Particolare cura deve essere posta nella stesura del piano di continuità operativa che deve comprendere, oltre ai sistemi informatici, ogni risorsa necessaria per svolgere i servizi istituzionali. Ad esempio, sfruttando la presenza di più sedi, il piano di continuità operativa potrà prevedere che, nel caso di inagibilità di una di esse, parte del personale e dei servizi si distribuisca opportunamente sulle altre sedi.

Soluzioni per amministrazioni di classe C

Nel caso di amministrazioni complesse, le soluzioni a basso costo – quali quelle basate sul mutuo soccorso – di fatto non sono praticabili. È invece possibile ricorrere a soluzioni basate su risorse condivise, purché tali soluzioni siano in grado di supportare l'intera gamma di servizi ritenuti essenziali, spesso basata su piattaforme elaborative eterogenee. La soluzione migliore, in questo caso, è ricorrere a servizi di *disaster recovery* specializzati o a centri di backup comuni, modulando, in ragione delle specifiche esigenze, la percentuale di risorse condivise e dedicate.
Nei sistemi complessi, le cause di fermo prolungato possono essere diverse, per cui nella scelta della soluzione è opportuno valutarne anche la versatilità.
In quest'ottica può essere opportuno considerare soluzioni basate su risorse dedicate "a caldo" o su adeguamenti architetturali (aumento della resilienza). Le soluzioni di quest'ultimo tipo di solito risultano particolarmente costose, o addirittura impraticabili, a causa dei vincoli dovuti ai sistemi esistenti. Può essere opportuno in questi casi adottare nel breve-medio periodo una soluzione basata su un centro di backup esterno e pianificare l'evoluzione dell'architettura verso sistemi maggiormente idonei ad assicurare la continuità operativa, prevedendo progressivi interventi di aggiornamento dei sistemi elaborativi e di comunicazione.
Analogamente, è opportuno che, in occasione dei rinnovi contrattuali, vengano introdotte clausole che tutelino l'amministrazione chiedendo ai fornitori di realizzare adeguati sistemi di continuità operativa.

Soluzioni per amministrazioni di classe D

Le amministrazioni appartenenti a questa categoria spesso dispongono di sistemi distribuiti con architetture complesse. In questo caso le soluzioni sono difficilmente generalizzabili, in quanto dipendono dal particolare contesto tecnico e organizzativo.
Nel caso di sistemi distribuiti, può essere opportuno seguire approcci diversi per la sede centrale e per le sedi periferiche. Per i servizi del sistema centrale, di solito conviene predisporre risorse alternative dedicate, ricorrendo a servizi specializzati o realizzando un proprio centro di backup.

Per le sedi periferiche è possibile seguire due strade:

- il ricorso, in caso di emergenza, alle risorse centrali (ordinarie o alternative);
- lo sviluppo di piani di continuità operativa specifici per le sedi periferiche.

La scelta dipende da considerazioni tecniche, ma è anche fortemente condizionata da aspetti organizzativi. La soluzione che prevede il backup a livello centrale è di solito più economica, ma limita l'autonomia delle sedi periferiche in quanto le vincola a operare congiuntamente al sistema centrale (spesso con processi sincroni). Inoltre, anche se i servizi di ripristino sono forniti dal sistema di backup centrale, occorrerà comunque che i piani prevedano opportune procedure a livello periferico per recuperare l'operatività in situazione di emergenza.
Nel caso si decida di predisporre specifici piani di continuità operativa per le sedi periferiche, si potranno utilizzare le soluzioni tipiche delle amministrazioni corrispondenti a tali sedi per dimensioni ed esigenze. Ad esempio il piano potrà prevedere una sorta di mutua assistenza tra sedi omologhe, eventualmente con il coordinamento del livello centrale (per maggiori dettagli si rimanda al paragrafo 1.4.3).
Per questa tipologia di amministrazione, anche al fine di individuare le scelte migliori, è sempre opportuno valutare interventi di razionalizzazione delle architetture (consolidamento), prevedendo eventualmente un percorso per adeguare progressivamente le soluzioni tecniche alle esigenze di continuità operativa.
In generale, la soluzione ottimale prevede più interventi di diverso tipo:

- il consolidamento delle architetture;
- l'aumento della resilienza ai guasti;
- il ricorso a risorse alternative esterne;
- l'adeguamento progressivo dei contratti per inserire opportune clausole di tutela dell'amministrazione.

Infine, considerando che i sistemi informatici complessi evolvono rapidamente, è opportuno prevedere una frequente attività di adeguamento del piano di continuità operativa e prove periodiche per valutare l'efficacia delle soluzioni intraprese.
A conclusione di questa descrizione di possibili soluzioni, si ritiene utile indicare, nella tabella seguente, le soluzioni di continuità maggiormente idonee per ogni classe di amministrazione.

	TIPOLOGIA DI AMMINISTRAZIONE			
	CLASSE A	CLASSE B	CLASSE C	CLASSE D
Mutuo soccorso	X	X		
Risorse condivise	X	X	X	
Risorse dedicate (a freddo)		X	X	X
Risorse dedicate (a caldo)			X	X
Adeguamento procedure salvataggio dati	X	X	X	X
Consolidamento o razionalizzazione		X	X	X
Aumento della resilienza		X	X	X
Servizi di disaster recovery	X	X		
Accordi per fornitura apparati	X			

Tabella 11

1.3. Disegno della soluzione

A valle della scelta della soluzione (o *delle* soluzioni) di continuità operativa più adeguata alle esigenze dell'amministrazione, vanno definite e progettate:

- le caratteristiche principali della soluzione nei diversi ambiti d'interesse (organizzazione, tecnologie, processi, risorse umane, ecc.);
- la strategia complessiva di gestione della continuità.

Vanno inoltre valutati nel dettaglio i costi delle soluzioni.

1.3.1 Identificazione dei gruppi di lavoro e dei comitati direttivi

Come prima indicazione, si osserva che è opportuno coinvolgere nelle attività di analisi e progettazione i responsabili dei servizi di cui va garantita la continuità.
Limitare il coinvolgimento ai responsabili delle funzioni informatiche è in generale un errore: occorre cooptare nei lavori tutti coloro che hanno responsabilità nella gestione dei processi che sottendono al servizio che si intende proteggere (intesi sia come processi "interni" sia come processi di interfaccia con gli "utenti" dell'amministrazione).
Come prima indicazione, l'identificazione delle persone da coinvolgere può essere effettuata partendo dall'organigramma dell'amministrazione (ad esempio si può decidere di coinvolgere i responsabili delle unità organizzative interessate al procedimento). Ma la scelta dipende anche delle caratteristiche (dimensioni, tipologia, grado di centralizzazione/decentralizzazione) dell'amministrazione stessa.
Un aspetto importante da considerare è la presenza o meno di attività o servizi critici affidati all'esterno. In questi casi, è opportuno il coinvolgimento nei lavori di referenti degli outsourcer, e ciò per consentire una progettazione di soluzioni di continuità efficaci e adeguate allo scopo. Vi sono infatti casi in cui la disponibilità di servizi critici per la missione di un'amministrazione non ricade sotto il controllo dell'amministrazione stessa (si pensi all'alimentazione elettrica o alla connettività telefonica). In questi casi, l'amministrazione ha la responsabilità del mantenimento di una continuità di servizio istituzionale pur non avendo il necessario controllo sui processi ad esso indispensabili.
Una volta individuate tutte le persone da coinvolgere, il passo successivo consiste nel definire le strutture organizzative che governeranno la continuità operativa nelle situazioni di emergenza. Queste strutture avranno in generale la responsabilità di:

- attivare e utilizzare le strutture per la continuità;
- assicurare la corretta esecuzione dei piani di continuità operativa;
- gestire il rientro a situazioni di normale operatività;
- coordinare le attività pianificate e le eccezioni.

Definire le strutture significa stabilire la composizione dei vari gruppi di lavoro, fissare le autonomie decisionali e i livelli gerarchici, assegnare compiti e responsabilità. Ciò dovrà essere fatto in maniera più o meno articolata a seconda delle dimensioni dell'amministrazione e della complessità dei processi da proteggere.
La composizione dei gruppi di lavoro è un compito complesso: spesso occorre infatti far collaborare persone che normalmente operano presso uffici diversi dell'amministrazione.

Le principali indicazioni, per la composizione dei gruppi, sono le seguenti:

- definire chiaramente il responsabile del gruppo e un suo eventuale sostituto;
- definire chiaramente il ruolo e le responsabilità di ciascun componente del gruppo;
- fare in modo che ciascun componente del gruppo abbia competenze adeguate al suo ruolo (evitare quindi di scegliere persone solo perché "in quel momento scariche da impegni");
- tener presente che, al momento del verificarsi di un'emergenza, il personale con skill critico può non essere reperibile, per cui è fondamentale disporre di una "soluzione di backup" anche per le persone.

Nel capitolo si descrive una possibile composizione delle strutture organizzative delegate a governare una soluzione di continuità operativa.

1.3.2 Disegno tecnico

Partendo dalla scelta della soluzione di continuità (effettuata nella fase precedente), in questa fase (definita in letteratura "disegno tecnico" o "progettazione") viene completata la trasformazione dei requisiti di continuità dell'amministrazione in specifiche della soluzione.
L'input di questa fase è dunque l'insieme dei requisiti di continuità (eventualmente diversi per i singoli servizi da proteggere), mentre l'output è un insieme di documenti di architettura tecnica della soluzione, comprendenti gli aspetti infrastrutturali e organizzativi della soluzione stessa.
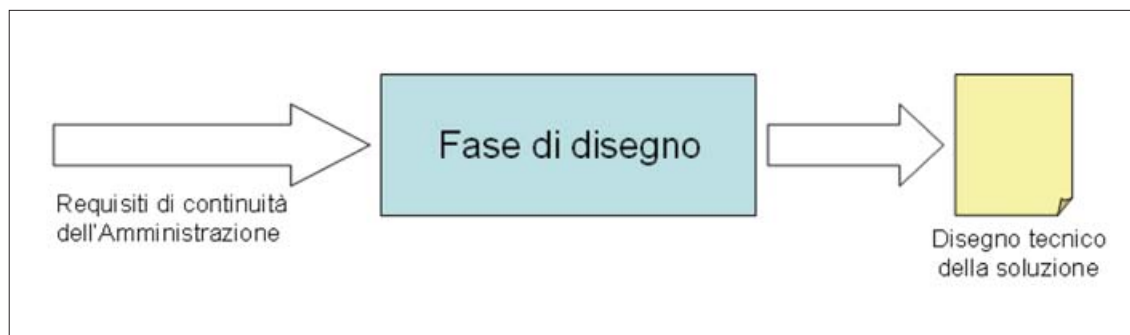
Figura 11

Come è stato detto nei paragrafi precedenti, i requisiti di continuità sono stati definiti a seguito dell'analisi del rischio e dell'analisi di impatto (BIA).
Una strutturazione tipica dei requisiti di continuità è:

- L'elenco dei servizi individuati come critici e, per ciascuno di essi:
  - L'elenco degli elementi hardware, software e organizzativi ("isola") che in condizioni di normale operatività concorrono alla sua erogazione;
  - la definizione del livello di servizio atteso in termini di RPO e RTO.

Poiché i requisiti di continuità sono in generale differenti sui vari processi e servizi da proteggere, è conveniente effettuare un'integrazione e un consolidamento di tali requisiti, con lo scopo di ottenere una coerenza della soluzione generale ed economie di scala.

Le specifiche della soluzione devono comprendere:

- l'elenco delle risorse da proteggere (questo elenco non coincide necessariamente con l'elenco di cui al punto precedente, più probabilmente sarà un suo sottoinsieme, ove vengono eliminate ridondanze e risorse non essenziali);
- la descrizione delle tecnologie da impiegare nella soluzione (con l'illustrazione di come tali tecnologie concorrono a garantire i requisiti di continuità attesi);
- la potenza, le caratteristiche, la configurazione e il dimensionamento dei componenti della soluzione (server, dispositivi di storage, dispositivi di rete, prodotti software, ecc.);
- la definizione delle regole di sicurezza (es. modalità di accesso ai sistemi e alle console) e di rete (es. convenzioni sull'indirizzamento IP e di routing, topologie di rete);
- nel caso la soluzione comprenda un sistema di backup, l'illustrazione di come il sistema di backup viene utilizzato in condizioni di emergenza e in condizioni di normale operatività[31];
- i modelli di accordi di supporto interni e di accordi di servizio con eventuali fornitori esterni.

Concettualmente, la fase di disegno tecnico di una soluzione di continuità operativa è del tutto assimilabile alla usuale fase di disegno e progettazione del progetto di un sistema informatico, anche se in teoria potrebbe portare solo alla definizione di modelli organizzativi e non alla realizzazione di una infrastruttura (o alla modifica della infrastruttura esistente). L'intera fase può essere condotta all'interno dell'amministrazione o demandata a un fornitore esterno. Nel secondo caso, è comunque opportuno il coinvolgimento di personale dell'amministrazione, sia a livello operativo che decisionale. I documenti di output di questa fase devono comunque essere approvati dall'amministrazione.
È opportuno, come del resto è raccomandato nella generalità dei progetti, utilizzare per la stesura dei documenti una notazione strutturata (accanto al semplice testo) o una serie di template standard. Ad esempio, utilizzando i formalismi dello UML, la componente tecnologica della soluzione può essere disegnata mediante un diagramma dei componenti e un diagramma di dispiegamento, mentre gli aspetti organizzativi (procedure di recupero, procedure di rientro, ecc.) possono essere descritti mediante diagrammi di attività.
È invece spesso inutile o fuorviante, perché in genere risultano di lettura non facile, includere nei documenti il disegno o la foto di particolari dispositivi tecnologici (dischi, SAN, linee dedicate ecc.).
Durante il disegno vanno esaminate varie alternative di progettazione, sempre all'interno della soluzione individuata al passo precedente della metodologia. Per ogni alternativa va effettuata una valutazione dei costi associati e una verifica dell'effettiva copertura dei requisiti.

[31] Col fine di evitare uno spreco di potenza elaborativa e di risorse, è opportuno progettare un uso del sistema di backup anche in condizioni di normale operatività (ad esempio, il sistema potrebbe essere usato come ambiente di sviluppo e test). L'illustrazione di tale uso alternativo sarà parte delle specifiche della soluzione.

Tra gli aspetti organizzativi che devono essere studiati durante la progettazione della soluzione vi è la definizione del processo di gestione dell'emergenza. Definire il processo significa:

- fornire criteri di valutazione dell'emergenza (es. numero di processi critici colpiti, portata dei danni);
- fornire scenari di riferimento e criteri di identificazione degli stessi;
- definire le modalità di dichiarazione dello stato di crisi;
- definire le modalità di ripristino della normale operatività.

1.3.3 Definizione delle modalità di test e manutenzione della soluzione

Parallelamente alla progettazione della soluzione di continuità operativa, devono essere progettate le modalità di test della soluzione stessa. È opportuno realizzare un piano di test formale, ove venga stabilita la modalità e la tempistica delle prove da condurre.
Scopo del test è verificare la validità nel tempo della soluzione di continuità (nei suoi aspetti tecnologici e organizzativi). Nella predisposizione dei test, si deve anche valutare l'opportunità di simulare situazioni di carico reali, al fine di verificare le soglie prestazionali critiche. Da questa definizione ne deriva che il piano di test deve prevedere prove ripetute e continuate nel tempo. A seguito dei risultati dei test, dovranno essere adottate eventuali azioni di correzione e adeguamento della soluzione. I test, in ogni caso, verificano sia l'adeguatezza della soluzione che la preparazione dei gruppi di lavoro coinvolti.
Sono possibili numerose modalità di test. In letteratura tecnica si individuano quattro principali tipologie, elencate in ordine crescente di complessità.

- **Verifica teorica**. È la metodologia più classica, e si riallaccia alle usuali tecniche di auditing e di validazione "su carta". Consiste nel condurre un'analisi di congruenza della soluzione, a cura degli autori stessi della soluzione o di esperti esterni.
- **Walk-through strutturato**. Si stabilisce uno scenario teorico di crisi, e i partecipanti al test (normalmente vengono coinvolti i responsabili dei vari gruppi e gli autori della soluzione da testare) percorrono ("walk-through") parallelamente le attività previste dal piano di continuità operativa. Lo scenario è reso noto prima della simulazione per consentire ai partecipanti di preparare e rivedere le attività assegnate a ciascuno. Nel corso del "walk-through" si verificano e documentano eventuali errori o carenze.
- **Tattico**. Consiste in una simulazione condotta come "gioco di guerra". Tutte le persone coinvolte (i responsabili dei vari gruppi di lavoro) sono chiamati a eseguire le attività previste dal piano di continuità operativa, comunicate in anticipo o a sorpresa, sulla base delle informazioni rese note dal coordinatore della simulazione. La simulazione deve riproporre il più realisticamente possibile lo scenario di crisi ipotizzato. In genere si utilizza un "orologio accelerato" per completare le attività di 3-4 giorni in un solo giorno lavorativo.
- **Simulazione**. In questo caso il test coinvolge l'intero personale dell'amministrazione o almeno il personale addetto all'area interessata dalla simulazione. Il test prevede l'esecuzione "in tempo reale" del piano di continuità operativa e la verifica delle procedure, dei sistemi di backup, dei sistemi alternativi di comunicazione, della mobilitazione dei gruppi di gestione dell'emergenza, del recupero di docu-

menti e dati. Condurre una simulazione di emergenza completa può avere un costo molto elevato. Per questo in genere si usano simulazioni semplificate (ad esempio limitate al ripristino della sola connettività di rete dalle sedi periferiche al centro di backup, oppure la sola ripartenza dei sistemi nel centro di backup con il collegamento al centro primario non attivo, ecc.).

Nel seguito, alcune indicazioni su come definire il piano dei test, e in particolare su come pianificare le simulazioni:

- le simulazioni devono essere progettate per simulare una "vera" condizione di emergenza, ricreando le conseguenze dell'evento peggiore nel peggior momento (ad esempio, l'improvvisa indisponibilità del CED primario durante l'orario di punta dei servizi erogati);
- per non rischiare di compromettere i dati di produzione per l'effettuazione delle simulazioni, dovranno essere predisposte copie dei dati che saranno cancellate al termine delle prove;
- è utile predisporre i test in moduli indipendenti, in modo tale da poter procedere comunque – anche in caso di fallimento del singolo modulo di test – alla verifica completa della soluzione. Questo approccio ha lo scopo di creare un clima di confidenza nel successo dell'operazione, in quanto tende ad allentare il livello di stress legato a un test del tipo "tutto o niente";
- nel caso la soluzione preveda un centro di backup, è necessario verificare e testare tutti quei processi e procedure che devono garantire, in condizioni di funzionamento normale del centro primario, le operazioni di allineamento dei due centri (copia remota dei dati, ecc.).

La manutenzione della soluzione di continuità non è comunque legata solo ai risultati dei test. Bisogna prevedere un processo di *change management* della soluzione di continuità, finalizzato a mantenerla aggiornata secondo le nuove situazioni che si vengono a creare, ad esempio:

- aggiunta di nuovi processi o servizi;
- variazioni delle configurazioni hardware o software;
- variazioni organizzative dell'amministrazione;
- nuovi requisiti di carattere legale o normativo.

1.3.4 Definizione del piano esecutivo di progetto

Relativamente alla soluzione di continuità individuata, durante questo passo viene redatto un piano degli interventi necessari per l'implementazione della soluzione. Tale piano includerà un elenco di attività da svolgere, con l'indicazione dei tempi necessari alla loro realizzazione (che concorrono a determinare la durata complessiva del progetto), nonché l'indicazione di massima delle quantità di risorse umane e finanziarie necessarie.
Tra le attività progettuali si troveranno ad esempio le seguenti:

- disegno di dettaglio della soluzione;
- approntamento delle procedure tecniche ed organizzative;

- allestimento degli spazi attrezzati;
- installazione e configurazione delle risorse elaborative;
- adeguamento dei prodotti software;
- attivazione di dispositivi di storage;
- collaudo;
- formazione degli utenti finali;
- gestione in esercizio.

Gli elementi fondamentali del piano esecutivo, analogamente a quanto avviene negli usuali progetti in campo IT, sono:

- il calendario dei rilasci;
- l'agenda delle attività, con le principali relazioni di dipendenza tra le macroattività, nonché l'evidenza dei momenti di controllo e di decisione.

Il calendario dei rilasci consiste:

- nella specificazione delle progressive realizzazioni del progetto (ad esempio previsioni di completamento di sottoinsiemi del sistema finale o di versioni successive dell'intero sistema o di sue parti);
- nella specificazione delle previsioni di completamento dei necessari prodotti intermedi.

L'agenda delle attività consiste invece nell'esplicitazione della sequenza e delle dipendenze tra le principali attività del progetto. È opportuno anche in questo caso utilizzare formalismi grafici quali, ad esempio, i diagrammi PERT. I momenti di controllo e di decisione saranno rappresentati tramite i "milestone" previsti dalla notazione del PERT. La sintesi generale del piano con l'indicazione delle scadenze previste potrà essere rappresentata tramite un diagramma di Gantt.
Nel corso della stesura del piano esecutivo si formalizzeranno le decisioni sull'eventuale segmentazione del progetto. Si deciderà cioè se la realizzazione avverrà:

- in una soluzione unica;
- in modo incrementale (per parti successive, ciascuna delle quali contiene un sottoinsieme delle funzionalità e dei servizi previsti; i requisiti della soluzione sono completamente definiti prima della realizzazione iniziale e non variano nel corso delle successive installazioni);
- in modo evolutivo (attività sperimentali o progetti pilota, in cui ogni versione può contenere tutte le funzionalità o un loro sotto-insieme; i requisiti del sistema possono essere variati tra due successive versioni, a causa di nuove informazioni).

In generale, l'approccio evolutivo è consigliato quando lo scenario progettuale (insieme dei requisiti) è incerto, mentre l'approccio incrementale è adeguato a situazioni complesse ma non incerte. Inoltre gli approcci incrementale o evolutivo sono da preferirsi quando ci sono tempi stretti, ossia se è necessario realizzare qualcosa al più presto.
Come principale indicazione, si raccomanda che la tempistica di attuazione del piano sia stabilita in modo da ridurre al massimo l'impatto sulla normale operatività dell'amministrazione.

È opportuno che il piano esecutivo contenga anche il riepilogo delle acquisizioni e delle realizzazioni previste nell'ambito del progetto, suddividendo le acquisizioni nelle seguenti categorie:

- sistemi elaborativi;
- apparati e servizi di rete (servizi di trasporto, apparecchiature...);
- software di base, d'ambiente e pacchetti applicativi;
- software applicativo ad hoc;
- servizi professionali.

Questo riepilogo sarà utile nel caso in cui le acquisizioni sono effettuate tramite gara: in questo caso, il riepilogo verrà utilizzato per la determinazione della base d'asta.
Dovranno essere definiti nel piano, infine:

- gli indicatori di qualità per il processo di realizzazione e i connessi servizi;
- le responsabilità progettuali, suddivise tra responsabilità dell'amministrazione e responsabilità dei vari fornitori coinvolti nel progetto. Ad esempio, tra le responsabilità dell'amministrazione potrebbero essere incluse:
  - la gestione dei fermi dell'operatività necessari alle attività del progetto;
  - la disponibilità del personale interno coinvolto nelle varie fasi progettuali;
  - la disponibilità dei sistemi e dei dati oggetto del progetto di continuità, nonché della relativa documentazione;

mentre tra le responsabilità dei fornitori possono esservi:
  - il rispetto dei tempi stabiliti;
  - la messa a disposizione di personale qualificato e di risorse elaborative;
  - una percentuale massima di turn-over tra i partecipanti al progetto, ecc.;
- le modalità di collaudo e i relativi criteri di superamento;
- le penali previste in caso di non rispetto dei livelli di servizio stabiliti.

1.3.5 Definizione dei programmi di informazione e addestramento

Oltre alle attività descritte nei precedenti paragrafi, durante la fase di disegno è opportuno progettare un piano di comunicazione per gli utenti (interni ed esterni) dell'amministrazione, con lo scopo di trasmettere le informazioni necessarie a tutti gli attori coinvolti nei possibili scenari d'emergenza.
Il piano di comunicazione potrà prevedere sessioni di presentazione per i diversi gruppi di lavoro, distribuzione di materiale illustrativo, manuali o altra documentazione. Successivamente potranno essere previste sessioni di aggiornamento e di mantenimento delle conoscenze. Uno scenario tipico prevede sessioni di aggiornamento con frequenza annuale per tutti i membri dei vari gruppi di lavoro.
La pianificazione della comunicazione e della formazione dovrà tenere conto della disponibilità di adeguati spazi (aule, sale riunioni, ecc.) e soprattutto della disponibilità del personale, da coinvolgere minimizzando l'impatto sulla normale operatività dell'amministrazione.
Per il personale tecnico incaricato della gestione delle componenti tecnologiche della soluzione di continuità (es. sistemi di storage, sito di backup) dovrà essere pianificato un

programma di istruzione e addestramento, finalizzato ad acquisire (o a completare l'acquisizione) delle competenze necessarie all'esercizio della soluzione di continuità.
Com'è noto, esistono numerose modalità di addestramento possibili (*training the trainer*, affiancamento, in aula, corsi on line, ecc.): l'amministrazione dovrà scegliere quale modalità è la più adeguata alle proprie esigenze, tenendo anche in questo caso in massima considerazione l'esigenza di limitare l'impatto sulla normale operatività.

1.4 IMPLEMENTAZIONE DELLA SOLUZIONE

1.4.1 REALIZZAZIONE DELL'INFRASTRUTTURA

In questa fase si svolgono le attività pianificate nella fase precedente, con riferimento alla realizzazione della infrastruttura tecnologica per la continuità.
Le procedure per la selezione del fornitore saranno, a seconda del contesto, la gara (nelle sue varie forme) o la trattativa privata. Sempre compatibilmente al contesto, potrebbe essere opportuno prevedere nella documentazione di gara che l'installazione, la messa in rete, la personalizzazione dell'infrastruttura acquisita e l'eventuale smaltimento di apparati e prodotti sostituiti dalle nuove acquisizioni, siano attività da svolgersi da parte del fornitore prescelto.
Le problematiche da affrontare in questa fase sono legate soprattutto alla gestione delle acquisizioni, agli aspetti finanziari delle stesse, alla tempistica delle consegne (ad esempio occorre curare che la consegna di apparecchiature avvenga a valle della disponibilità dei locali che dovranno ospitarle).
In generale, per uno svolgimento efficace di questa fase, l'indicazione è seguire le regole e le best practice valide nelle usuali attività di realizzazione di infrastrutture informatiche, non esistendo specificità particolari legate al tema della continuità operativa.

1.4.2 ATTIVAZIONE DEI MECCANISMI DI COPIA DATI E CONFIGURAZIONI

In questa fase dovranno svolgersi le attività pianificate durante la fase di disegno, con riferimento ai meccanismi di backup e di configurazione della componente tecnologica della soluzione.
Per lo svolgimento di queste attività non è sempre necessario attendere che sia stata completata la realizzazione dell'infrastruttura: in generale, la schedulazione progettuale può prevedere l'anticipazione di alcune attività sulle parti di infrastruttura già disponibile, e la successiva estensione via via che il resto dell'infrastruttura viene completato: ciò può consentire una contrazione dei tempi di progetto.
Le problematiche da affrontare in questa fase sono legate al tipo di soluzione tecnologica scelta: per maggiori dettagli, si rimanda alla descrizione delle varie tecnologie esistenti sul mercato presente nel capitolo 5.

1.4.3 REDAZIONE DEL PIANO DI CONTINUITÀ OPERATIVA

Il piano di continuità operativa (di seguito, "Piano") è, come definizione generale, il documento che guida un'amministrazione nella gestione e mediazione dei rischi cui essa è soggetta. Il Piano definisce ed elenca le azioni da intraprendere prima, durante e dopo una condizione d'emergenza per assicurare la continuità del servizio. Nell'ambito del presente studio, per Piano si intende precisamente il piano di continuità operativa per i sistemi informatici di un'amministrazione.

Si tratta di un documento di interesse generale per i dirigenti dell'amministrazione e, in particolare, per i responsabili della continuità dei servizi erogati agli utenti. Oltre al personale dirigente, sono destinatari di questo documento anche tutti coloro che hanno ruolo di progettazione, sviluppo, implementazione e gestione dei sistemi informatici. Se tra questi ci sono fornitori esterni, l'amministrazione dovrà aver cura di richiedere loro l'adesione, nello svolgimento del lavoro commissionato, ai criteri e alle indicazioni del Piano.
Tra i destinatari sono da annoverarsi anche gli utenti finali dei sistemi informatici dell'amministrazione, almeno per quanto riguarda:

- l'impatto, sul loro lavoro, delle procedure operative definite nel Piano;
- le aspettative di ripristino, a fronte di un evento critico, dei servizi da loro fruiti.

Il Piano è un documento che va necessariamente:

- compreso e recepito da tutto il personale coinvolto;
- aggiornato periodicamente (o su eventi specifici) anche in funzione dell'evoluzione del sistema informatico;
- allineato a possibili mutamenti delle politiche di sicurezza dell'amministrazione.

Obiettivi e contenuti del piano di continuità operativa
Il principale obiettivo del Piano è massimizzare l'efficacia delle operazioni in risposta a un'emergenza. Per ottenere questo risultato è necessario pianificare gli interventi previsti in modo ben definito, prendendo in considerazione le singole fasi in cui sono generalmente raggruppate le azioni da intraprendere in seguito al verificarsi dell'emergenza. Esse sono:

- notifica al personale deputato alla valutazione del danno e attivazione delle risorse destinate al conseguente ripristino;
- ripristino dei servizi attraverso misure di disponibilità alternativa dei servizi stessi, ad esempio riavviando il servizio in un sito alternativo;
- in caso di interruzione prolungata, attivazione delle procedure per far fronte a un'indisponibilità prolungata nel tempo delle risorse necessarie all'erogazione dei servizi;
- ritorno alla normale operatività, cioè alle condizioni precedenti al verificarsi dell'emergenza.

Nel Piano vengono anche:

- pianificate le attività (trasversali alle fasi testé definite) di coordinamento con eventuali strutture esterne che concorrono all'erogazione dei servizi, compresi eventuali fornitori;
- assegnati i ruoli e le responsabilità;
- documentati tutti gli aspetti tecnici che consentono di eseguire le operazioni di gestione dell'emergenza.

Il Piano è tanto più efficace quanto più è "ritagliato a misura" dell'amministrazione che deve utilizzarlo, cioè quanto più risponde ai requisiti di continuità espressi dall'amministrazione stessa. Tuttavia, più il Piano è dettagliato, meno esso risulta versatile: nella redazione del Piano si devono bilanciare precisione e flessibilità.

Ad esempio, anziché definire una dettagliata serie di vincoli sull'aggiornamento del Piano, è meglio stabilire la frequenza di revisione in funzione della maturità organizzativa e tecnologica dell'amministrazione. In caso di struttura stabile e di piattaforme tecnologiche consolidate, la frequenza potrebbe essere bassa, mentre se l'amministrazione sta ristrutturando la propria organizzazione o sta modificando i propri sistemi informatici, la frequenza di revisione del Piano dovrà essere alta.
Il Piano deve essere strutturato in modo da fornire subito l'idea e l'indirizzo da seguire anche a chi non ha familiarità con la tematica. Ove possibile, è preferibile realizzare delle check-list e/o procedure da eseguire passo passo.
Per quanto riguarda i contenuti, il Piano dovrebbe riportare, in una prima sezione introduttiva, i risultati ottenuti dalla fase di BIA, descrivere la strategia di continuità adottata e fornire tutte le necessarie informazioni a supporto (ad esempio, le informazioni relative allo stato corrente dei beni da proteggere). In una seconda sezione, il Piano dovrebbe riportare il dettaglio delle operazioni da realizzare nelle singole fasi previste e i relativi riferimenti organizzativi.
Nell'appendice B è presentato l'indice e i contenuti tipici di un possibile Piano (da considerare a titolo d'esempio, e che richiede adattamenti ai casi specifici e alle situazioni reali).

1.5 GESTIONE E MANUTENZIONE

La gestione della soluzione di continuità richiede una manutenzione costante di tutti i suoi componenti, tecnici e organizzativi, in modo che essa rimanga comunque allineata all'evoluzione del sistema informativo e della struttura organizzativa dell'amministrazione.
Per realizzare questo obiettivo è necessario che, durante l'esercizio, la soluzione di continuità sia sottoposta a prove periodiche, che:

- verifichino l'impatto di eventuali trasformazioni del contesto;
- assicurino l'efficienza della soluzione;
- mantengano la sensibilità al tema della continuità operativa;
- contribuiscano ad addestrare il personale coinvolto.

Le attività di gestione comprendono inoltre l'aggiornamento e la corretta diffusione della documentazione, sia per gli aspetti tecnici che per quelli organizzativi.
Per riassumere, si può affermare che durante l'esercizio della soluzione di continuità si devono mantenere:

- un'infrastruttura tecnologica efficiente e aggiornata;
- processi e procedure adeguate e aggiornate;
- personale addestrato e sensibilizzato;
- procedure e sistemi di protezione dei dati correnti e archiviati.

L'attuazione di quanto descritto dovrà essere specificata nel Piano che, come detto, è il documento principale per la gestione della soluzione di continuità durante tutta la sua vita.
Le attività necessarie per la manutenzione della soluzione di continuità si possono suddividere in due categorie: manutenzione ordinaria e manutenzione straordinaria.

La manutenzione ordinaria comprende gli interventi che comportano modifiche puntuali al contenuto del Piano e non modifiche sostanziali del contenuto o della sua struttura. Normalmente, comprende:

- l'aggiornamento dell'inventario delle risorse;
- l'aggiornamento, automatico o manuale, delle procedure di allineamento e di ripartenza del sito alternativo;
- le prove periodiche di funzionamento del Piano;
- le modifiche dei recapiti del personale delle strutture organizzative coinvolte;
- l'apertura di nuovi servizi verso la clientela o l'aggiornamento architetturale di servizi già esistenti.

La manutenzione straordinaria comprende gli interventi di aggiornamento derivanti da ogni variazione (tecnologica, organizzativa o logistica) che possa in qualche modo invalidare l'efficacia della soluzione, come, per esempio:

- l'adozione di nuove piattaforme tecnologiche nel sistema;
- l'estensione della continuità operativa a nuovi servizi;
- l'outsourcing di attività o variazioni dell'organizzazione o dei ruoli dell'amministrazione.

1.5.1 Esecuzione dei test

Le attività di test hanno l'obiettivo di verificare che la soluzione tecnico-organizzativa posta in essere sia adeguata al raggiungimento degli obiettivi di continuità definiti dall'amministrazione.
Nella fase di esecuzione dei test vengono attuate le verifiche e gli interventi pianificati in fase di definizione del piano dei test (vedi paragrafo 1.3.3), secondo le modalità, l'approccio e la tempistica stabilite.
Come indicazione pratica, si suggerisce l'utilizzo, ove possibile, di specifiche check-list, orientate a testare i diversi aspetti della soluzione di continuità da verificare. Di seguito vengono forniti, a titolo d'esempio, alcuni schemi e check-list applicabili ai tipici ambiti di test: documentazione, gestione dei nastri, siti alternativi.

Test della Documentazione

Questi test hanno l'obiettivo di verificare la completezza e la correttezza degli aspetti documentali della soluzione di continuità. I documenti da prendere in considerazione si possono suddividere, per praticità, in due categorie:

- Documenti generali:
  - documentazione a supporto della *Business Impact Analysis*;
  - schema dei processi da proteggere;
  - documentazione tecnica varia;
  - mappa della sede con la dislocazione fisica dei team coinvolti;
  - formulari (es. autorizzazioni, agende, riferimenti, ecc.);
- Documenti di pianificazione:
  - obiettivi e responsabilità dei team coinvolti;

– procedure operative di ciascun team;
– descrizione delle attività di ciascun team;
– procedure e componenti di basso livello:
  - procedure operative;
  - *job scheduling*;
  - elenco e descrizione delle procedure ordinarie (*application runbook*);
  - elenco e descrizione delle procedure alternative (*disaster recovery fallback runbook*)[32];
  - schemi di configurazione di rete;
  - procedure di escalation;
  - lista dei contatti;
  - registro dei *security log*;
  - manuale del sito alternativo;
  - configurazione dei sistemi;
  - requisiti di storage;
  - descrizione delle attività di *change control*;
  - sequenza per il ripristino delle applicazioni;
– aggiornamenti del Piano.

Test dei nastri

La verifica della gestione in luoghi esterni di nastri di dati è di fondamentale importanza per il ripristino del sistema. Le principali verifiche devono riguardare i seguenti aspetti:

- revisione regolare delle procedure di backup;
- salvataggio giornaliero di file critici e contestuale conservazione fuori sede;
- lista degli specifici nastri necessari per ciascuno step di ripristino;
- verifica che i tempi di ripristino dei nastri dalla sede esterna siano compatibili con il RTO;
- verifica delle procedure di autorizzazione all'accesso ai nastri di ripristino;
- documentazione del processo di acquisizione dei nastri di ripristino;
- test del processo di acquisizione dei nastri di ripristino;
- procedure documentate e relativi test per:
  – inizializzazione dei disk drive;
  – restore system (reload);
  – reboot from stand-alone backup;

[32] L'elenco delle procedure ordinarie e alternative sono documenti cartacei che riportano le procedure che devono essere seguite in condizioni ordinarie o eccezionali. Tipicamente tali documenti descrivono le procedure per la partenza dei sistemi e della rete, l'arresto dei medesimi, il monitoraggio, la gestione di richieste quali il montaggio di dispositivi contenenti materiale archiviato e le procedure che devono essere seguite nel caso che insorgano problemi non previsti.

– esecuzione della ripartenza;
– ripristino delle altre librerie;
– system StartUp;
– ripristino delle applicazioni;
– ripristino dei data base.

TEST DEI SITI ALTERNATIVI

Nel seguito vengono indicati, sotto forma di domande cui il test deve rispondere, i principali aspetti oggetto di verifica in funzione delle diverse possibili tipologie di siti alternativi, cioè in funzione della tipologia di soluzione di continuità adottata.

Sito per ripristino a freddo (*cold site*)

- La dislocazione fisica del sito è nota a tutti i team coinvolti?
- È stata realizzata una visita fisica al sito da parte di tutti?
- Sono stati eseguiti test di accesso al sito e di evacuazione dallo stesso?
- Il sito è attualmente equipaggiato con tutte le attrezzature che è previsto debbano essere presenti?
- Sono state testate le attrezzature per verificare che siano perfettamente funzionanti?
- Ci sono procedure per avviare il ripristino dell'operatività nel sito?
- Il sito è dotato di sistemi di sicurezza? Le persone coinvolte sanno come attivarlo/utilizzarlo?
- Ci sono cavi, telefoni, modem, fax, etc, del tipo giusto e in quantità tale da garantire i requisiti di ripristino? Sono correttamente funzionanti?
- Lo spazio a disposizione per l'operatività complessiva è sufficiente?
- Ci sono le mappe dei piani e gli schemi di reti e sistemi?
- Ci sono le procedure per l'evacuazione di emergenza del sito?
- I dispositivi anti-incendio rispettano gli standard e sono stati verificati periodicamente?
- Tutti questi aspetti sono documentati in un manuale del sito? Una copia di tale manuale è a disposizione nel sito?
- Il sito risponde a tutti i requisiti di ripristino per gli aspetti di rete e di comunicazione?
- Presso il medesimo sito sono dislocate altre entità? Se sì, queste altre entità sono totalmente isolate dal nostro ambiente di ripristino?
- È stato attivato un processo per testare regolarmente l'efficace funzionamento di ogni attrezzatura?

Sito per ripristino a caldo (*hot site*) di fornitore esterno

- Le dotazioni del sito (sistemi, periferiche, reti di comunicazione,…) sono compatibili con l'attuale dotazione del sito di produzione?
- Le dotazioni del sito dedicate al ripristino sono correttamente dimensionate e configurate? È disponibile un elenco aggiornato di tutte le configurazioni?
- Il sito dispone di funzionalità di *tape library*?
- Le dotazioni del sito sono verificate regolarmente da personale specialistico professionale?
- Quali procedure sono poste in essere per assicurare che le dotazioni siano allineate allo stato corrente?
- Quali test sono stati eseguiti sulle apparecchiature di cui è dotato il sito?
- Sono stati verificati tutti i requisiti di *licensing* del software che girerà nel sito alternativo durante il periodo di ripristino?

Sito per ripristino a caldo di proprietà dell'amministrazione

- Nel sito sono disponibili sistemi per la continuità operativa?
- I sistemi sono dimensionati adeguatamente per consentire il ripristino (capacità CPU e dischi, tape drive ecc. adeguati ai requisiti utente)?
- Lo staff tecnico è a conoscenza di quali ambienti software rimuovere e come lasciare sufficiente spazio ai processi di ripristino?
- Sono state definite e documentate le procedure per il ripristino?
- Sono state definite e documentate le procedure di pulizia per i sistemi di ripristino quando al termine dell'emergenza si procederà al ritorno alla normale elaborazione?

2. Analisi costi/benefici

2.1 Metodo di analisi economica

Come già specificato nel precedente capitolo, uno degli elementi fondamentali nella scelta della soluzione di continuità operativa è la determinazione dei costi e il confronto di questi con i benefici attesi.
L'analisi dei costi e dei benefici delle soluzioni inizia sin dalla fase di studio del contesto ed è effettuata, in particolare, nel corso della *Business Impact Analysis*. L'analisi economica si sviluppa, poi, durante l'esame delle soluzioni possibili.
Il metodo di analisi economica proposto si basa sul confronto tra i costi delle diverse soluzioni ammissibili ed i costi che l'amministrazione deve sostenere in caso di evento che provoca l'interruzione dei servizi, costi che saranno diversi a seconda della soluzione di continuità operativa attivata. In generale, più costosa è la soluzione di continuità scelta (e migliori le sue caratteristiche in termini, ad esempio, di RTO e RPO), più limitati saranno i danni economici derivanti dall'interruzione del servizio. Coerentemente con quanto illustrato al paragrafo 1.1.3, anche attraverso la figura schematica di confronto tra costi della soluzione e costi dell'indisponibilità, l'analisi economica ha come obiettivo la scelta del miglior compromesso tra costi da sostenere per la realizzazione della soluzione e costi generati dalla assenza di servizio. Questa analisi deve ovviamente tenere conto delle risorse economiche disponibili per la realizzazione e la gestione della soluzione di continuità. Si deve considerare anche che esistono soluzioni idonee solo per eventi eccezionali (interruzione totale del servizio provocata, in genere, da disastri naturali, attentati, ecc.) e soluzioni "ad ampio spettro", cioè soluzioni che prevedono l'uso delle risorse aggiuntive anche in occasione di piccoli disservizi o di eventi pianificati (ad esempio, interventi di manutenzione ordinaria). Nel primo caso, l'analisi economica è semplificata in quanto i benefici sono riconducibili soltanto ai minori oneri da sostenere in caso di disastro. Nel secondo caso, oltre a questi, si dovranno considerare anche gli effetti benefici su periodi di interruzione minori.
Per effettuare l'analisi economica deve essere definito un periodo di tempo sufficientemente lungo (qualche anno) cui la stessa analisi va riferita. A quel periodo devono essere riportati gli investimenti da effettuare e i costi correnti. Per lo stesso intervallo temporale deve essere stimata la probabilità che si verifichino gli eventi che portano all'interruzione del servizio.

2.2 I costi delle soluzioni di continuità

I costi per la continuità operativa possono essere suddivisi nelle seguenti tipologie:

a) costi necessari per la predisposizione della soluzione (stesura del piano ed approntamento delle infrastrutture di ripristino);

b) spesa che occorre sostenere per mantenere la soluzione efficace nel tempo (costi di personale per la gestione del piano e le prove periodiche, eventuali costi per la trasmissione dei dati verso il centro di backup, ecc.);
c) costi che devono essere sostenuti per l'attivazione della procedura di continuità operativa;
d) costi necessari alla fase di rientro, cessato il periodo di emergenza.

La valutazione dei costi deve essere riportata al periodo di riferimento scelto. Per ciascuna soluzione in esame si deve perciò:

- stimare i costi di tipo a);
- calcolare i costi di tipo b) nel periodo di riferimento;
- stimare, nel periodo di riferimento, la distribuzione e la tipologia degli eventi per i quali può essere opportuno utilizzare una soluzione di continuità operativa e stimare il costo per ciascun evento in assenza di una soluzione di continuità operativa e in presenza di ciascuna soluzione prevista; questi due elementi (numero di occorrenze degli eventi e costo di gestione di ciascun evento) consentono di stimare i costi di tipo c).

Per quanto riguarda i costi di tipo d), in prima istanza, si può stimare che i costi relativi al ripristino della normale operatività siano equivalenti in presenza o in assenza di una soluzione di continuità operativa. In effetti il costo di ripristino è generalmente inferiore in presenza di un piano di continuità operativa, ma questo minor costo è in parte compensato dai maggiori costi necessari all'avvio del piano ed alla gestione dell'emergenza.

2.3 I costi del disservizio

Il calcolo dei benefici di una soluzione di continuità per una pubblica amministrazione, cioè il calcolo dei minori oneri sostenuti in situazioni di emergenza, deve prendere a riferimento la comunità a cui i servizi sono destinati. I costi del disservizio dovranno dunque essere valutati tenendo conto delle perdite per i cittadini e le imprese che correntemente utilizzano i servizi dell'amministrazione. A questi costi occorre aggiungere i maggiori costi per l'amministrazione causati dal disservizio, come quelli per il recupero del lavoro perso o per mancati o ritardati introiti.
I costi del disservizio possono essere suddivisi in:

- perdita di produttività per cittadini ed imprese;
- perdita di produttività per l'amministrazione;
- mancati o ritardati introiti.

2.3.1 La perdita di produttività per cittadini ed imprese

Le perdite economiche dovute al degrado o all'assenza dei servizi istituzionali costituiscono una parte sostanziale dei costi imputabili ad un eventuale disservizio del sistema informativo. Infatti il completo subentro dell'informatica nei processi amministrativi tradizionali comporta, oltre che una maggiore efficienza, una sostanziale dipendenza dai servizi ICT,

tanto che una loro discontinuità può condizionare pesantemente la produttività di cittadini ed imprese. L'effetto non riguarda solo i servizi offerti in forma elettronica (cosiddetti servizi di e-government), ma anche quelli che gli utenti percepiscono come servizi tradizionali ma che oramai si basano su una infrastruttura completamente informatizzata.
Il costo della perdita di produttività per cittadini ed imprese dipende significativamente dalla natura dei servizi erogati. Se l'interruzione dei servizi ha una durata limitata, il danno economico consiste nel tempo speso invano per ottenere il servizio (ad esempio per ottenere un certificato).
Una valutazione grossolana del danno potenziale può essere condotta stimando il valore statistico di produttività persa dal soggetto interessato da un disservizio. Secondo tale criterio, la perdita di produttività di un'ora provoca, per ciascun soggetto interessato dal disservizio, un danno pari a circa 33 euro[33]. Con tale ipotesi, ad esempio, se il numero medio di soggetti che utilizzano i servizi di un'amministrazione nel corso di una giornata è pari a 10.000 e ciascuno di essi perde in media un'ora per effetto del disservizio, il danno economico complessivo per la collettività è pari a circa 300.000 euro. Ovviamente questa stima è del tutto indicativa, poiché la perdita effettiva dipende fortemente dal settore in cui il disservizio si verifica.
Il danno economico per la perdita di produttività cresce più che linearmente nel tempo, per il fatto che il numero degli utenti che tentano invano di ottenere il servizio si incrementa progressivamente per il ripetersi dei tentativi[34].
Il danno economico descritto tiene conto solo della mancanza di produttività per il tempo speso inutilmente, è stato cioè stimato nell'ipotesi che il cittadino o l'impresa possa comunque ottenere il servizio in tempo utile, dopo averlo richiesto più volte. Questa assunzione è verosimile se la durata del disservizio è contenuta (dell'ordine di ore). Man mano che il periodo del disservizio aumenta, ai danni dovuti alla perdita di tempo possono aggiungersi altre perdite causate dal non poter svolgere processi indispensabili per l'attività produttiva. Perdite economiche di questo tipo possono essere dovute a: blocco di alcune attività[35], mancati affari, mancati introiti, perdita di competitività, ecc. Ad esempio l'assenza di alcuni servizi pubblici cruciali può comportare per un'azienda problemi analoghi a quelli che possono derivare dal blocco del proprio sistema informatico.
La stima di questi ulteriori danni è alquanto complessa poiché dipende dalla natura dei servizi erogati, dalle caratteristiche del bacino di utenza e dal particolare periodo temporale. In generale le perdite di questo tipo aumentano esponenzialmente con il passare del tempo.
Bisogna infine tenere presente che, di solito, il periodo di disservizio per cittadini ed imprese è maggiore dell'effettivo periodo di fermo dell'amministrazione in quanto il ritorno alla situazione normale richiede lo smaltimento del carico di lavoro arretrato che si è generato in assenza dei servizi informatici.

---

[33] Per calcolare tale valore si è considerata la quota parte di PIL per unità di lavoro (dati ISTAT 2005) e la si è rapportata al periodo considerato supponendo che in un anno si lavori in media 8 ore per 220 giorni.

[34] Se ciascun utente continuasse a richiedere il servizio con costanza, il numero dei soggetti contemporaneamente coinvolti dal disservizio crescerebbe linearmente ed il danno per la perdita di produttività crescerebbe con andamento quadratico. Questa condizione in realtà non si verifica per vari motivi, ma il danno in ogni caso cresce in modo più che lineare.

[35] Si consideri ad esempio il ritardo nell'avvio di una attività economica per l'impossibilità di ottenere un permesso o un certificato a causa dell'indisponibilità di un servizio pubblico.

Figura 12 - Costo del disservizio per cittadini ed imprese

Il diagramma di figura 12 rappresenta un esempio di andamento del costo per collettività derivante dall'interruzione dei servizi resi da un'amministrazione di grosse dimensioni. Si è ipotizzato che i servizi vengano utilizzati quotidianamente da circa 5.000 utenti e che, per effetto dell'assenza di uno di essi, ciascun utente sprechi un'ora di tempo. Si è inoltre immaginato che il numero medio degli utenti "non serviti" si incrementi ogni giorno del 10% per effetto dei tentativi ripetuti. Al costo dovuto alla mancanza di produttività si è aggiunto un ulteriore costo con andamento esponenziale per tenere conto dei danni indiretti dovuti al disservizio (blocco di attività, mancati introiti, ecc.). Tale ulteriore costo è stato valorizzato ipotizzando che, dopo 10 giorni di fermo, le perdite indirette eguagliano quelle dovute alla mancanza di produttività.

2.3.2 La perdita di produttività per l'amministrazione

L'assenza di continuità operativa comporta una perdita economica per l'amministrazione in conseguenza del fermo forzato dei dipendenti. Questa perdita si concretizza in un costo addizionale per il recupero dei procedimenti sospesi a causa del disservizio[36].

[36] Questa voce di costo è spesso trascurata da chi ritiene che l'amministrazione non abbia scadenze nell'espletamento delle pratiche e dunque il disservizio sia esclusivamente a carico di cittadini ed imprese. Fortunatamente questo modo di intendere il servizio pubblico è sempre meno attuale (cfr. art. 3 del Codice dell'amministrazione digitale), per cui in caso di disservizio le amministrazioni sono tenute a recuperare velocemente gli arretrati per mantenere il livello di servizio atteso.

Il costo associabile a questa perdita di produttività dipende dalla capacità di recupero dei procedimenti amministrativi interrotti. Se il disservizio avviene in un periodo di basso carico di lavoro per l'amministrazione ed ha una durata relativamente breve (dell'ordine di ore), il lavoro arretrato può essere recuperato senza costi addizionali. Se la durata dell'interruzione supera una determinata soglia, che è funzione del carico di lavoro corrente, occorrerà ricorrere al lavoro straordinario e la perdita economica può essere calcolata con riferimento agli importi contrattuali per le maggiori prestazioni. Occorre comunque tenere presente che il lavoro straordinario non può superare una determinata percentuale del lavoro ordinario, pertanto il lavoro perso viene di solito recuperato in un tempo pari a 2-4 volte il periodo di interruzione. Per questo motivo, se l'interruzione ha una durata considerevole (ad esempio maggiore di una settimana) può essere necessario ricorrere a personale aggiuntivo, oppure a servizi esterni, per recuperare in tempo utile gli arretrati.
La perdita di produttività per l'amministrazione può essere valorizzata considerando una percentuale del costo di personale. Per una stima di carattere orientativo, si può considerare un costo per maggiori prestazioni relativo ad un periodo pari a 3 volte il periodo di disservizio, ipotizzando una spesa aggiuntiva per il personale pari al 30%. Nel grafico che segue si è riportato, a titolo di esempio, il costo per un'amministrazione con 3.500 dipendenti tenendo conto che solo una parte di essi sarà impegnata nel recupero delle attività sospese (si è ipotizzato un valore pari al 50%). Per valorizzare il costo, si è supposto che i dipendenti percepiscano uno stipendio medio annuo lordo pari a 27.000 euro.
Nell'esempio si è ipotizzato che, per recuperare il lavoro arretrato a seguito di fermi superiori ad una settimana, si debba ricorre a servizi di una società esterna con un costo pari a 20.000 euro per ogni giorno da recuperare.
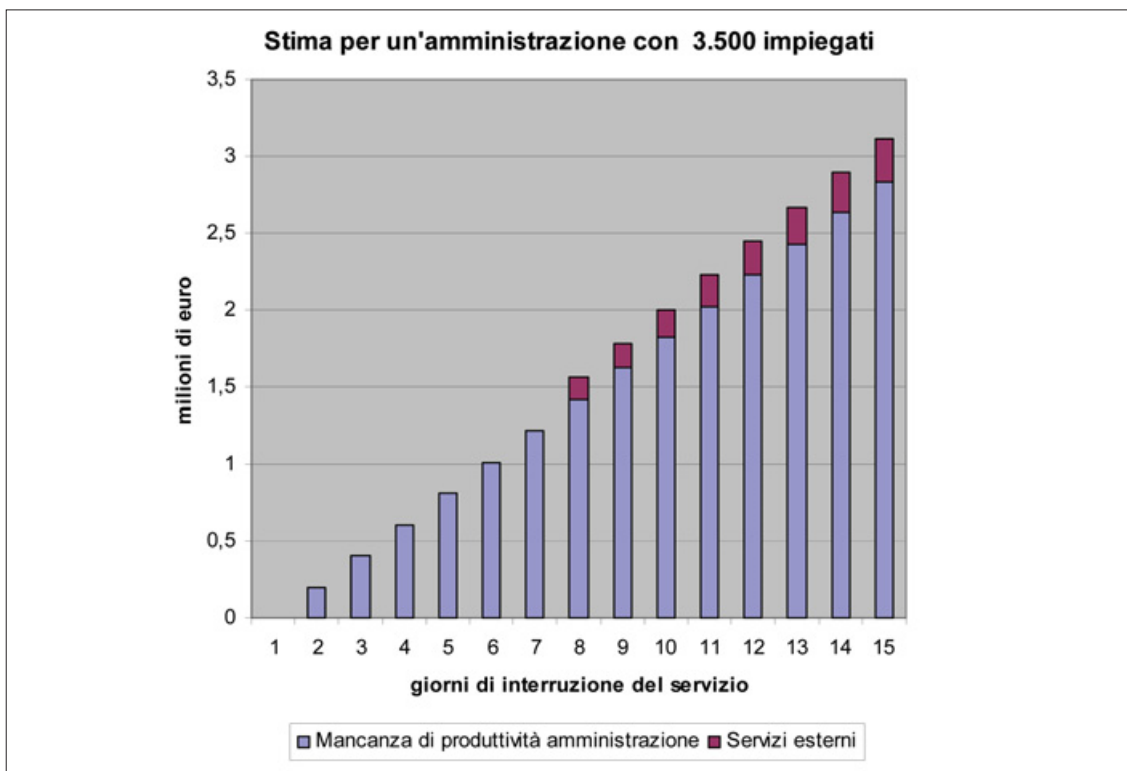
Figura 13 - Costo per perdita di produttività dell'amministrazione

2.3.3 MANCATI O RITARDATI INTROITI

Questa voce di costo è certamente significativa per il settore privato, ma ha un valore marginale nel caso di una pubblica amministrazione. Infatti in genere l'assenza dei servizi pubblici non esonera cittadini ed imprese dal pagamento degli importi dovuti, pertanto il disservizio genera semplicemente un ritardo negli introiti e, di conseguenza, la perdita degli interessi.
Una effettiva perdita economica può aver luogo nei seguenti casi:

- quando, a seguito di un evento disastroso, l'amministrazione perde i dati necessari per richiedere gli importi dovuti;
- nei casi in cui, per sanare situazioni dovute a disservizi di durata elevata, vengono condonati i tributi dovuti.

I possibili danni per mancati o ritardati introiti dipendono significativamente dalla tipologia di amministrazioni. Nel caso di amministrazioni pubbliche che non hanno una connotazione economica, tali perdite si possono ritenere trascurabili rispetto alle altre voci descritte.

2.4 CONFRONTO DEI COSTI

La tabella seguente mostra, in modo schematico, un esempio delle diverse tipologie di costo che devono essere prese in considerazione e nel confronto tra tre scenari:

- assenza di soluzioni di continuità;
- presenza di una soluzione attivata solo in caso di eventi eccezionali;
- presenza di una soluzione a largo spettro.

Si sono ipotizzati, oltre al caso di disastro che si stima possa avvenire solo una volta nel periodo di riferimento, altri due possibili eventi che la soluzione a largo spettro è in grado di gestire. In calce alla tabella sono spiegate le notazioni utilizzate.

VOCE DI COSTO	TIPO DI COSTO	ASSENZA DI CONTINUITÀ OPERATIVA	SOLUZIONE 1 (EVENTI ECCEZIONALI)	SOLUZIONE 2 (AMPIO SPETTRO)
Costi della soluzione				
Predisposizione	Una tantum	–	CP1	CP2
Mantenimento	Annuo	–	CM1 * aa	CM2 * aa
Attivazione della continuità operativa per evento disastroso	Per evento	–	CD1	CD2
Attivazione della continuità operativa per evento a	Per evento	–	–	Ca2 * na
Attivazione della continuità operativa per evento b	Per evento	–	–	Cb2 * nb

(segue)

Costi dei disservizi				
Perdita per evento disastroso (per utenti + per amministrazione + per mancati introiti)	Per evento	PD	PD1	PD2
Perdita per evento a (per utenti + per amministrazione + per mancati introiti)	Per evento	Pa * na	Pa * na	–
Perdita per evento b (per utenti + per amministrazione + per mancati introiti)	Per evento	Pb * nb	Pb * nb	–

aa: numero di anni di riferimento
CP1 e CP2: costi di predisposizione delle soluzioni 1 e 2
CM1 e CM2: costi di mantenimento annui delle soluzioni 1 e 2
na e nb: numero di eventi di tipo a e di tipo b previsti nel periodo di riferimento
CD1 e CD2: costi di attivazione delle procedure di emergenza
Ca2 e Cb2: costo di attivazione delle procedure, nella soluzione 2, per gli eventi a e b
PD, PD1 e PD2: perdite per disastro in caso di assenza di soluzione, soluzione 1 e soluzione 2
Pa e Pb: perdite per occorrenza degli eventi a e b

Tabella 12

Anche con le semplificazioni introdotte, la scelta della soluzione in funzione dei costi è un processo complesso. Di solito il processo di progettazione porta ad individuare le caratteristiche delle soluzioni esclusivamente in base ai requisiti di continuità e soltanto nella fase finale emerge l'intero costo della soluzione. Se tale costo viene ritenuto non adeguato agli obiettivi di continuità operativa, è spesso necessario ripetere la fase di progettazione fino ad individuare, per approssimazioni successive, il miglior bilanciamento tra requisiti e costi.
Si osserva infine che la scelta della soluzione di continuità operativa non può essere motivata solo da considerazioni economiche: vincoli di natura normativa o particolari condizioni al contorno possono far propendere per determinate soluzioni a prescindere da considerazioni di natura economica. Tutte le indicazioni fornite devono pertanto essere mediate con altre considerazioni di natura strategica.

2.5 I BENEFICI NON ECONOMICI

I vantaggi della continuità operativa non consistono solo nella riduzione dei costi per il disservizio, ma riguardano anche la fiducia nei servizi informatici e, di conseguenza, la possibilità di diffonderli ed utilizzarli proficuamente.
È infatti in atto un processo di modernizzazione del Paese che si basa sullo sviluppo della società dell'informazione. Tale sviluppo comprende diverse iniziative rivolte sia all'incremento di efficienza della Pubblica Amministrazione, sia al miglioramento dei rapporti tra cittadini ed istituzioni (tra queste iniziative si citano l'alfabetizzazione digitale, la diffusione della firma elettronica e delle carte per l'accesso ai servizi in rete, lo sviluppo della larga banda, la posta elettronica certificata, ecc.). Tutte queste iniziative presuppongono che gli utenti (cittadini ed imprese) abbiano una sufficiente fiducia nel mezzo informatico.
A tal proposito si osserva che diversi studi hanno evidenziato come la fiducia degli utenti condizioni fortemente l'uso dei servizi e determini addirittura l'economia del settore che

si basa su tali servizi[37] . Nel caso dei servizi di e-government la fiducia degli utenti è un elemento fondamentale che può abilitarne o bloccarne lo sviluppo.
L'affidabilità, la sicurezza e la disponibilità dei servizi sono elementi che concorrono a determinare la fiducia degli utenti. Il legame tra questi elementi e la fiducia è complesso e mentre i primi variano gradualmente in funzione di diversi fattori, la fiducia degli utenti assume di regola solo due stadi (presente o non presente). Un disservizio prolungato[38], tale da comportare la perdita di fiducia da parte degli utenti, vanificherebbe i benefici derivanti dallo sviluppo dei servizi informatici e comporterebbe un danno indiretto molto elevato. Al contrario, la fiducia nella disponibilità dei servizi pubblici, suffragata dalla presenza diffusa di soluzioni di continuità operativa, rappresenta un elemento di stimolo all'utilizzo dei servizi informatici che comporta modernità ed efficienza.

2.6 I BENEFICI INDIRETTI PER L'AMMINISTRAZIONE

La realizzazione di una soluzione di continuità operativa comporta diversi benefici che, anche se non relazionabili con l'obiettivo di ridurre i tempi di fermo, possono comunque essere utili all'amministrazione.
Innanzitutto il percorso di progettazione della soluzione richiede attività di rilevazione ed inquadramento dei procedimenti che sono molto utili per la razionalizzazione e l'ammodernamento dei processi e dell'amministrazione. La fase realizzativa comporta inoltre la revisione ed ottimizzazione dell'architettura attraverso i processi di consolidamento. I vantaggi di questi interventi architetturali sono molteplici e vanno dalla riduzione della spesa informatica al miglioramento dei livelli di servizio.
L'organizzazione della continuità operativa prevede la creazione di strutture e di relazioni (ad es. comitato di crisi) finalizzate alla gestione dell'emergenza. Queste relazioni, consolidate attraverso le prove periodiche, di solito sono utili anche in situazioni di emergenza non necessariamente correlate a problemi di continuità operativa. In altre parole, un'organizzazione che ha una soluzione di continuità operativa di solito affronta meglio anche altri problemi di sicurezza. Inoltre le prove di simulazione dell'emergenza spesso consentono di rilevare problemi o incongruenze relative al sistema in esercizio.
Infine, quando si dispone di un sistema alternativo dedicato, tale sistema può essere utilizzato anche per attività di manutenzione ordinaria, incrementando significativamente il livello di disponibilità dei servizi informatici.

2.7 L'ANALISI DEI COSTI DELLE SOLUZIONI DI CONTINUITÀ OPERATIVA

Il problema della valutazione dei costi di una soluzione di continuità operativa è alquanto complesso per l'elevato numero di fattori che entrano in gioco. I costi dipendono infatti dalle caratteristiche della soluzione che possono essere espresse con più parametri:

1. RTO (tempo di ripartenza);

[37] Si cita a tal proposito il documento OCSE "Economics of trust in the information economy: issues of identity, privacy and security".

[38] Si osservi che, con lo sviluppo dei servizi on line, la tolleranza al disservizio diventa sempre più bassa. Un utente di Internet ritiene inaccettabile che un sito sia "fuori linea" per più di un'ora e può perdere la fiducia dopo poche ore di fermo.

2. RPO (massimo intervallo di transazioni perse);
3. versatilità della soluzione (cioè possibilità di utilizzo anche in condizioni ordinarie);
4. qualità e sicurezza dei servizi in condizioni di emergenza;
5. probabilità di recupero (ossia probabilità che la soluzione, eventualmente condivisa da più organizzazioni, sia efficace anche al verificarsi contemporaneo di più eventi disastrosi);
6. tempo massimo di permanenza in condizioni di emergenza.

Queste variabili sono tra di loro indipendenti e, anche se alcune combinazioni non sono significative, è teoricamente possibile "costruire" la soluzione scegliendo il valore più opportuno per ciascun parametro.
Nel seguito viene fornita una breve descrizione di come i principali elementi di costo vengano influenzati dai parametri della soluzione.

2.7.1 La predisposizione del piano di continuità operativa

Il costo relativo alla predisposizione del piano di continuità è funzione della complessità dell'amministrazione ed è invariante rispetto ai parametri espressi. La predisposizione del piano richiede un impegno in risorse professionali molto variabile a seconda della tipologia di organizzazione e dipende sia dalle dimensioni che dalla complessità dell'amministrazione stessa. L'impegno può variare da qualche giorno per organizzazioni molto semplici fino a diversi mesi per amministrazioni particolarmente complesse.

2.7.2 Il consolidamento delle architetture

Il consolidamento è considerato un'attività propedeutica ad una soluzione di continuità operativa. Il costo dipende dall'architettura di partenza e dalla complessità del sistema informatico. Il livello di consolidamento incide principalmente sul tempo di ripartenza e sul massimo intervallo di transazioni perse.

2.7.3 L'impianto della soluzione

I costi d'impianto sono relativi principalmente alla predisposizione del sistema alternativo per il ripristino. I costi sono dovuti ai prodotti informatici aggiuntivi (sistemi, apparati di rete, software) e, in maggiore misura, alle infrastrutture logistiche ed ai servizi presso il sito alternativo.
La spesa per il sistema alternativo incide sul tempo di ripartenza, la versatilità della soluzione, la qualità e sicurezza dei servizi in condizioni di emergenza, la probabilità di recupero ed il tempo massimo di permanenza in condizioni di emergenza.
Il costo dipende dai seguenti fattori:

- i parametri di qualità citati;
- la complessità e la dimensione del sistema alternativo;
- il livello di condivisione con altre organizzazioni.

Generalmente, si ritiene che questa voce di costo, a parità di tipologia di soluzione, sia direttamente proporzionale alla spesa per il sistema informatico.

2.7.4 L'allineamento dei dati

Al costo per l'allineamento dei dati concorrono principalmente le spese di trasporto dei nastri di backup o, in alternativa, i canoni per i servizi di trasmissione dati.
Questo costo assume un valore discontinuo a seconda della soluzione ed è in relazione con il massimo intervallo di transazioni perse (RPO), il numero di utenti serviti, il tempo di ripartenza e la probabilità di recupero[39].

2.7.5 La gestione della soluzione

Questa voce di costo è dovuta alle seguenti attività continuative:

- manutenzione hardware del sistema alternativo;
- aggiornamento software del sistema alternativo;
- canoni e consumo per il sito alternativo;
- gestione quotidiana del sito alternativo;
- gestione periodica (prove);
- manutenzione e adeguamento delle soluzioni.

Questa spesa incide principalmente sulla qualità e sicurezza dei servizi in condizioni di recupero e può essere calcolata come una percentuale dell'intero costo per la continuità operativa (10%-30%).

2.7.6 Relazione tra parametri e costi delle soluzioni

Come abbiamo visto, il costo per la soluzione di continuità operativa è funzione di molti parametri.
Generalmente, per affrontare il problema, si considera sufficiente prendere in considerazione solo uno di questi parametri, ritenuto più rilevante nel caso in esame, nell'ipotesi che gli altri siano ad esso correlati. Ad esempio, se viene scelto il tempo di ripartenza RTO si ipotizza che, a fronte di tempi ripartenza ridotti, sia necessario garantire una minima perdita di dati (basso valore di RPO), così come a fronte di tempi di ripartenza più elevati si ipotizza che sia sostenibile una maggiore perdita di dati. Se queste relazioni non sono ritenute accettabili, si dovrà costruire un modello più complesso basato su entrambi i parametri.
La figura 14 mostra un'ipotesi di andamento dei costi della soluzione di continuità al variare del parametro RTO. La figura 14 mette comunque in evidenza che altri fattori, riportati nella figura stessa, possono modificare, anche notevolmente, i costi della soluzione.

2.8 Un esempio di valutazione delle soluzioni

2.8.1 I costi delle soluzioni di continuità

La determinazione dei costi di una soluzione di continuità operativa può avvenire solo a seguito di un progetto che tenga conto dei vincoli e delle condizioni a contorno. Tra le

[39] La probabilità di recupero aumenta con la distanza tra il centro primario ed il centro alternativo e tale distanza condiziona i costi per l'allineamento dei dati.
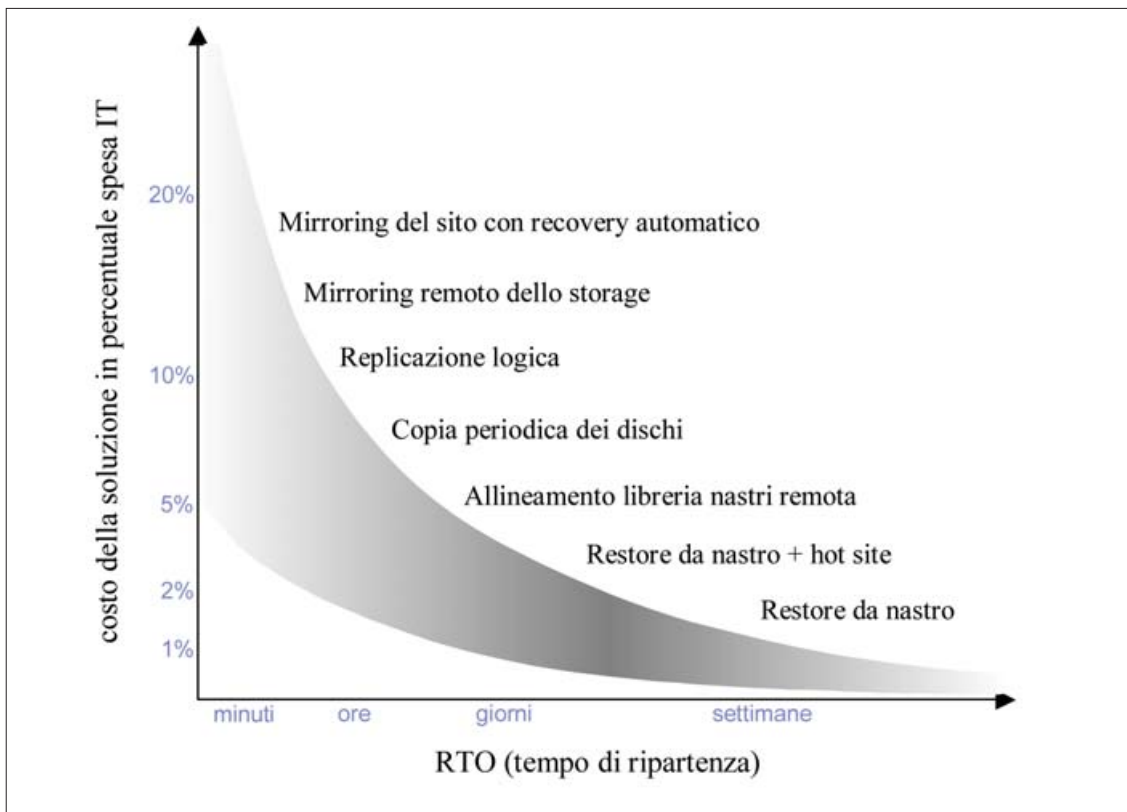
Figura 14 - Relazione tra il tempo di ripartenza ed il costo della soluzione

condizioni al contorno che possono condizionare significativamente i costi ci sono l'architettura del sistema informativo, la dislocazione geografica dell'amministrazione ed i costi di comunicazione.
Nell'esempio sviluppato si suppone che i costi siano funzione dei seguenti fattori:

- tempo di ripartenza dei servizi informatici (RTO) espresso in giorni;
- spesa informatica dell'amministrazione;
- numero di dipendenti dell'amministrazione;
- livello di condivisione del sistema alternativo.

Si suppone quindi che gli altri parametri (ad esempio l'RPO) siano direttamente correlati a quelli presi in considerazione.
L'amministrazione esempio ha 3.500 dipendenti e sostiene una spesa annua per l'informatica pari ad 20 milioni di euro.
Per il calcolo dei costi della soluzione si è considerato:

- un costo una tantum per la stesura del piano pari a 140.000 euro (175 giorni persona);
- un costo annuo[40] di impianto (risorse alternative) variabile tra 6,5 milioni di euro e 26.000 euro in funzione del tempo di ripartenza e del livello di condivisione delle risorse;

[40] La cifra si riferisce al canone di noleggio o all'ammortamento dei costi per l'acquisizione delle risorse.

- un costo annuo di allineamento dati funzione del tempo di ripartenza per valori inferiori ai tre giorni e trascurabile negli altri casi (il valore massimo è pari a 1 milione di euro per anno)[41];
- un costo annuo di gestione pari al 20% dei costi esposti.

Il costo relativo alle attività di consolidamento non è stato valorizzato in quanto non direttamente relazionabile alle caratteristiche della soluzione: si è ritenuto che questa omissione non infici il modello in quanto le attività di consolidamento dovrebbero essere condotte a prescindere dall'adozione di una soluzione di continuità operativa.
La figura 15 mostra la relazione tra il costo annuale per la continuità operativa ed il tempo di ripartenza nelle due ipotesi seguenti:

- centro alternativo completamente dedicato all'amministrazione;
- centro alternativo condiviso tra 10 amministrazioni.
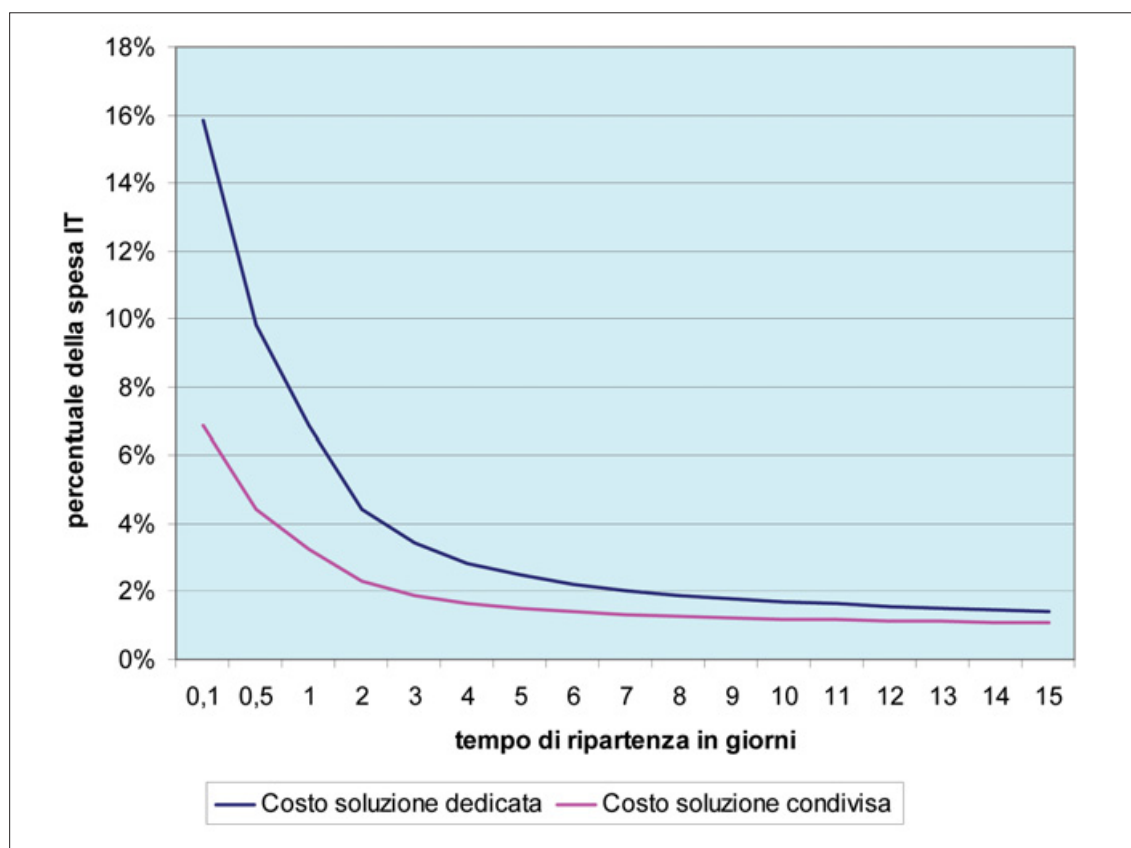
Figura 15 - Simulazione dei costi per la continuità operativa con modello matematico

2.8.2 I BENEFICI DELLE SOLUZIONI PER L'EMERGENZA

Le soluzioni di questo tipo sono una sorta di assicurazione nei confronti di eventi eccezionali e, di norma, vengono utilizzate solo in tali circostanze. Di solito, al verificarsi di

[41] Si è supposto che le soluzioni con tempo di ripartenza superiore a 3 giorni si basino su un allineamento tramite nastri, il costo è dunque quello relativo al trasporto dei medesimi, trascurabile rispetto agli altri costi.

un evento critico ma non calamitoso, si evita di avviare il piano di continuità operativa per non incorrere nei costi addizionali. Se il problema cresce di gravità con il trascorrere del tempo può capitare che, pur disponendo di una soluzione idonea a fornire il servizio presso un sito alternativo, si temporeggi nella speranza di risolvere il problema in tempi brevi, interrompendo il servizio anche per giorni. L'analisi costi/benefici può dunque essere condotta considerando un unico evento di gravità tale da consigliare l'avvio del piano di continuità operativa. Nell'esempio si è ipotizzato che un evento di questo tipo si verifichi in media ogni 4 anni.
Per effettuare il confronto con i costi delle soluzioni definiti nel paragrafo precedente si è così operato:

- per rendere coerenti i valori delle ordinate dei due grafici, i costi della soluzione sono stati rapportati a 4 anni quadruplicando tutti i costi ricorrenti;
- si è ipotizzato che, per effetto degli arretrati da recuperare, il tempo di disservizio sia doppio rispetto al tempo di ripartenza. Quindi il costo di disservizio corrispondente ad un determinato valore di RTO è stato calcolato prendendo a riferimento un periodo di disservizio doppio (ad esempio, il costo di disservizio corrispondente al valore delle ascisse di 4 giorni è stato calcolato prendendo a riferimento un periodo di disservizio di 8 giorni).

Nel grafico è evidenziata la curva dei costi per il disservizio e le curve dei costi della soluzione di continuità operativa nelle due ipotesi:

- soluzione dedicata;
- soluzione condivisa tra 10 amministrazioni.

Tra i costi associabili al disservizio non sono stati considerati eventuali danni indiretti per le imprese e le perdite per mancati o ritardati introiti.
Prendendo a riferimento una delle due curve (ad esempio quella relativa alla soluzione dedicata), per ogni valore del tempo di ripartenza dovremo considerare due costi:

- quello relativo alla soluzione di continuità operativa;
- il costo dovuto al disservizio residuo che la soluzione comporta.

La soluzione economicamente più conveniente è quella in cui la somma di questi due costi è minima.

2.8.3 I BENEFICI DELLE SOLUZIONI AD AMPIO SPETTRO

Nel caso di soluzioni ad ampio spettro, il modello di simulazione deve essere modificato per tenere in conto il differente approccio al problema della continuità operativa.
Le soluzioni di questo tipo si configurano infatti come adeguamenti dell'architettura di sistema che hanno l'obiettivo di incrementare la disponibilità dei servizi sia in condizioni ordinarie che in presenza di eventi particolarmente critici.
I costi per questo tipo di soluzione possono essere suddivisi in:

1. costi per incrementare la ridondanza degli apparati;
2. costi dovuti alla distanza tra gli apparati ridondati (remotizzazione).
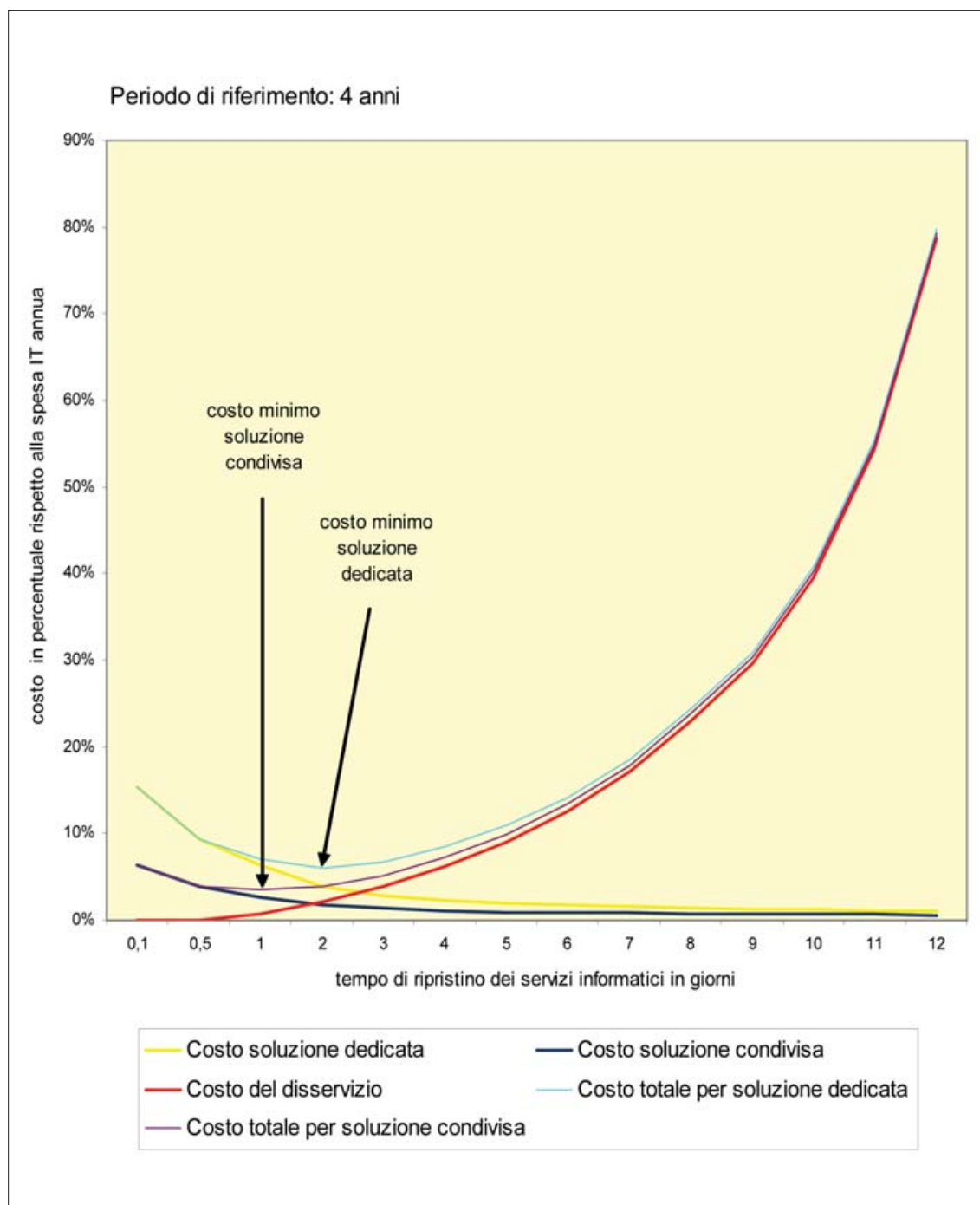
Figura 16 - Analisi dei costi e dei benefici delle soluzioni per l'emergenza

La prima tipologia di costi è correlata alla disponibilità dei sistemi, attiene cioè alla qualità del servizio piuttosto che alle problematiche di continuità operativa.
Per tale motivo, nell'analisi di costi e benefici non è corretto considerare tale voce di costo; è invece opportuno prendere in considerazione i costi dovuti all'esigenza di garantire la continuità anche a seguito di eventi particolari che bloccano l'operatività del sito.

Quest'ultimi sono a loro volta composti da:

a) costi per il sito alternativo;

b) costi per i servizi di comunicazione.

I costi di tipo a) possono essere assenti se l'amministrazione dispone di più sedi e fa in modo che i sistemi siano ridondati su due sedi, ciascuna delle quali può fungere da sito di ripristino per l'altra: in questo caso i costi maggiori sono quelli per l'allineamento dei sistemi.
Per quanto concerne i costi per il disservizio, occorre prendere in considerazione tutte le interruzioni che, statisticamente, si verificano nel periodo di riferimento.
A mero titolo di esempio si è ipotizzato che nel periodo di quattro anni, preso a riferimento nei casi precedenti, si verifichino mediamente le interruzioni riportate nella seguente tabella.

NUMERO DI INTERRUZIONI NEL PERIODO DI 4 ANNI	DURATA DELL'INTERRUZIONE IN ORE
96	0,5
32	1
16	3
8	12
4	24

Tabella 13

Il costo per il disservizio causato da queste interruzioni può essere valorizzato con i criteri esposti nel capitolo 2.3, ipotizzando che, nel solo caso di un'interruzione di 24 ore, il periodo di effettivo disservizio sia di due giorni per effetto della coda di arretrati.
Con tale ipotesi si ottengono i costi seguenti[42]:

NUMERO DI INTERRUZIONI NEL PERIODO DI 4 ANNI	DURATA MEDIA DELL'INTERRUZIONE IN ORE	COSTO DEL DISSERVIZIO IN MILIONI DI EURO
96	0,5	1,09
32	1	0,73
16	3	1,09
8	12	1,46
4	24	2,48
TOTALE		**6,86**

Tabella 14

Confrontando questi costi con quelli della specifica soluzione (principalmente dovuti ai servizi di comunicazione) è possibile effettuare un'analisi di tipo economico. A puro titolo illustrativo, si ripropone il grafico di figura 16 prendendo in considerazione anche i costi appena elencati.

[42] I costi sono stati calcolati prendendo a riferimento un'amministrazione con 3.500 dipendenti che offre servizi in media a 5.000 utenti al giorno; non sono stati considerati i costi per mancati servizi alle imprese e per mancati o ritardati introiti.

Nel grafico è stata mantenuta la curva relativa ai costi associabili ad una soluzione dedicata, basata cioè su un sito alternativo dedicato. Tale curva tuttavia è poco significativa per il fatto che, come si è detto, non è corretto imputare alla continuità operativa anche costi architetturali che servono per migliorare la qualità del servizio.
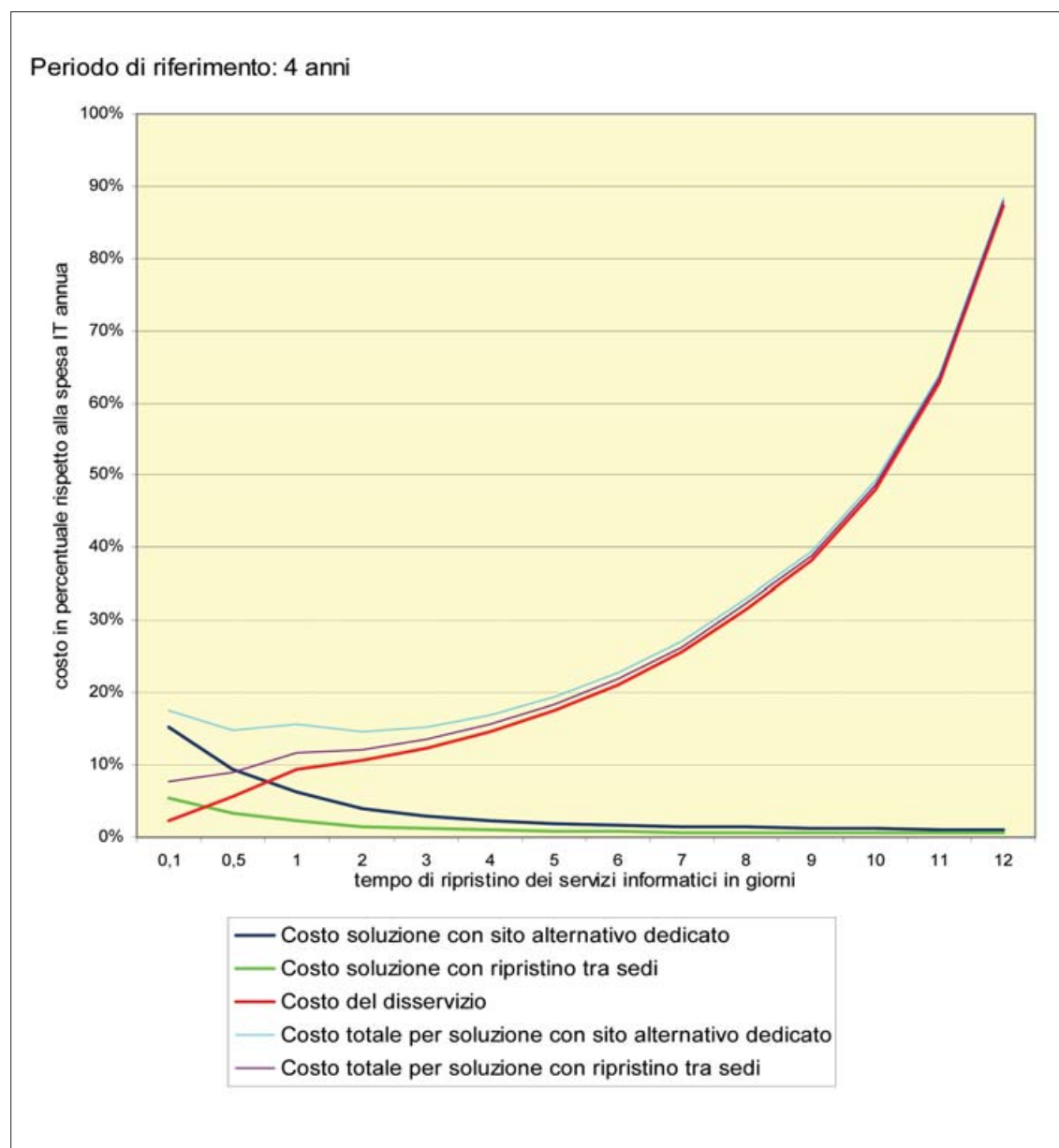
Figura 17 - Analisi dei costi e dei benefici delle soluzioni ad ampio spettro

Per un'analisi più significativa è stata evidenziata anche la curva dei costi relativi alla soluzione in cui i sistemi sono ridondati su due sedi, ciascuna delle quali può fungere da sito di ripristino per l'altra (soluzione con ripristino tra sedi)[43].

In questo caso, come può desumersi dal grafico, la soluzione economicamente più conveniente è quella che assicura un ripristino veloce.

2.9 CONCLUSIONI

L'esercizio di analisi dei costi e benefici per la continuità operativa ha lo scopo di agevolare la scelta della soluzione attraverso considerazioni di natura economica, ma da solo non consente di determinare i costi reali del progetto né di compiere scelte di natura tecnica. Si ricorda a tal proposito che, quando l'amministrazione ritiene di scegliere la soluzione economicamente più vantaggiosa, il "vantaggio" va misurato non solo in termini economici, ma anche tenendo conto dei benefici non direttamente monetizzabili e di considerazioni di natura strategica.
Ciò premesso, l'analisi appena svolta consente comunque di trarre alcune importanti conclusioni.
La prima riguarda l'importanza di predisporre in ogni caso una soluzione di continuità operativa: i costi per la collettività associabili a periodi prolungati di disservizio sono così elevati che vale sempre la pena adottare una soluzione che li riduca significativamente.
Per quanto concerne la soluzione, occorre scegliere tra due approcci diversi: soluzioni più economiche, ma idonee solo per eventi eccezionali, oppure soluzioni ad ampio spettro. Le due classi di soluzioni non sono direttamente confrontabili in quanto influiscono diversamente sulle caratteristiche di qualità e sicurezza dell'intero sistema informatico.
Nel caso della prima categoria di soluzioni, secondo il modello proposto non è economicamente conveniente predisporre sistemi con tempi di ripartenza (RTO) ridottissimi, ma è preferibile orientarsi su scelte che permettono di ripristinare il sistema informatico in tempi variabili tra 1 giorno ed una settimana.
Il discorso cambia per le soluzioni ad ampio spettro che, con particolari scelte architetturali, risultano convenienti anche per valori di RTO inferiori.
La scelta ottimale dipende ovviamente dai compiti istituzionali dell'amministrazione e dovrà tenere conto delle altre considerazioni espresse nel presente documento.

[43] In questo caso sono stati considerati i seguenti costi: predisposizione della soluzione, allineamento dei dati e gestione.

3. Organizzazione delle strutture di gestione della continuità operativa

Questo capitolo propone consigli e indicazioni su come creare e organizzare, all'interno di una amministrazione pubblica, le strutture incaricate di gestire le problematiche della continuità operativa.
Alcuni concetti che verranno espressi nel seguito sono, in parte, già stati anticipati nel capitolo dedicato alla metodologia. In questa sede, però, essi verranno esaminati sotto un diverso profilo, e approfonditi sottolineandone l'aspetto organizzativo piuttosto che quello metodologico.

3.1 Missione

La struttura organizzativa preposta a gestire le problematiche di continuità operativa all'interno di un'amministrazione ha per definizione la missione di:

- predisporre tutte le misure necessarie per ridurre l'impatto di un'emergenza;
- mettere a disposizione risorse alternative a quelle non disponibili;
- governare il sistema durante l'emergenza;
- gestire il rientro alla normalità.

In condizioni ordinarie, la suddetta struttura pianifica e definisce le attività necessarie ad affrontare le emergenze, adotta opportuni strumenti e adeguate soluzioni tecnologiche, fa in modo che i suoi componenti abbiano un'elevata sensibilità nei confronti delle attività e delle capacità richieste affinché il processo di mantenimento della continuità operativa abbia successo.
In condizioni di emergenza la struttura assicura l'ordinato svolgimento di una molteplicità di azioni, a partire dalla gestione delle operazioni tecniche alle comunicazioni.

3.2 Criteri per la dichiarazione di emergenza

In condizioni di emergenza risulta di fondamentale importanza riconoscere immediatamente il carattere dell'evento critico e reagire in tempo con adeguate contromisure.
Non tutti gli eventi critici evolvono in un disastro (per una definizione puntuale di disastro, vedi il glossario). Non è quindi sempre necessario attivare i processi definiti per il ripristino: ciò dipende dall'impatto dell'evento che si è verificato sui servizi critici dell'amministrazione.

È opportuno, perciò, che chi opera e vigila sulla corretta erogazione dei servizi critici disponga di criteri oggettivi sulla base dei quali:

- valutare la portata dell'evento e la sua effettiva gravità;
- scegliere se innescare o meno i processi definiti per il ripristino.

A titolo di esempio, vengono di seguito elencate alcune condizioni (in termini di conseguenza di un evento) che determinano senz'altro la necessità di attivare i processi di ripristino:

- distruzione delle infrastrutture del CED dell'amministrazione;
- impossibilità di accedere ai locali del CED o di controllare il funzionamento degli apparati in esso ospitati per un tempo indeterminato;
- impossibilità di erogare servizi a un'utenza considerevole o significativa;
- impossibilità di controllare l'esercizio delle applicazioni, con grande indeterminatezza sia per l'estensione del danno che per la sua durata.

Come ulteriore indicazione, è fortemente consigliabile predisporre e aggiornare l'elenco dei servizi e delle applicazioni critiche (vedi quanto detto a proposito della BIA, paragrafo 1.1.2). Nel citato elenco saranno specificate, per ogni elemento dell'elenco, le condizioni di attenzione, superate le quali si deve attivare la struttura dedicata alla continuità. Le condizioni di attenzione possono ad esempio essere espresse in termini di:

- numero massimo di segnalazioni di malfunzionamento eseguite dagli utenti del servizio in un dato intervallo temporale;
- intervallo di tempo massimo in cui il sistema risulta inoperoso (oltre tale durata, probabilmente c'è un problema sulla rete o altrove che impedisce agli utenti di accedere al sistema).

3.3 COINVOLGIMENTO DEI VERTICI DELL'AMMINISTRAZIONE

Per garantire l'efficacia della soluzione di continuità, in genere è necessario che:

- la struttura organizzativa definita e in generale l'intera soluzione siano condivisi, promossi e sostenuti, con un chiaro mandato, dai massimi vertici dell'amministrazione;
- quanto progettato venga promulgato attraverso atti e documenti specifici;
- vengano istituite ufficialmente le strutture organizzative previste, allocando le risorse umane ed economiche necessarie.

3.4 ARTICOLAZIONE DELLA STRUTTURA PER LA CONTINUITÀ

È opportuno che la struttura organizzativa definita per la continuità abbia responsabilità e compiti ben definiti, e che possieda ampia autonomia decisionale e disponibilità di utilizzare risorse straordinarie.

È senz'altro preferibile che il governo dell'emergenza sia affidato a un'unica struttura organizzativa, seppure articolata in componenti, caratterizzata da un unico responsabile e da un solo piano di azione complessivo.
Per le grandi amministrazioni e gli enti si propone un'articolazione quale quella rappresentata nella figura seguente. Per realtà organizzative più piccole, viceversa, alcuni dei gruppi descritti potrebbero coincidere, e la struttura risultante potrebbe essere più snella e meno articolata.
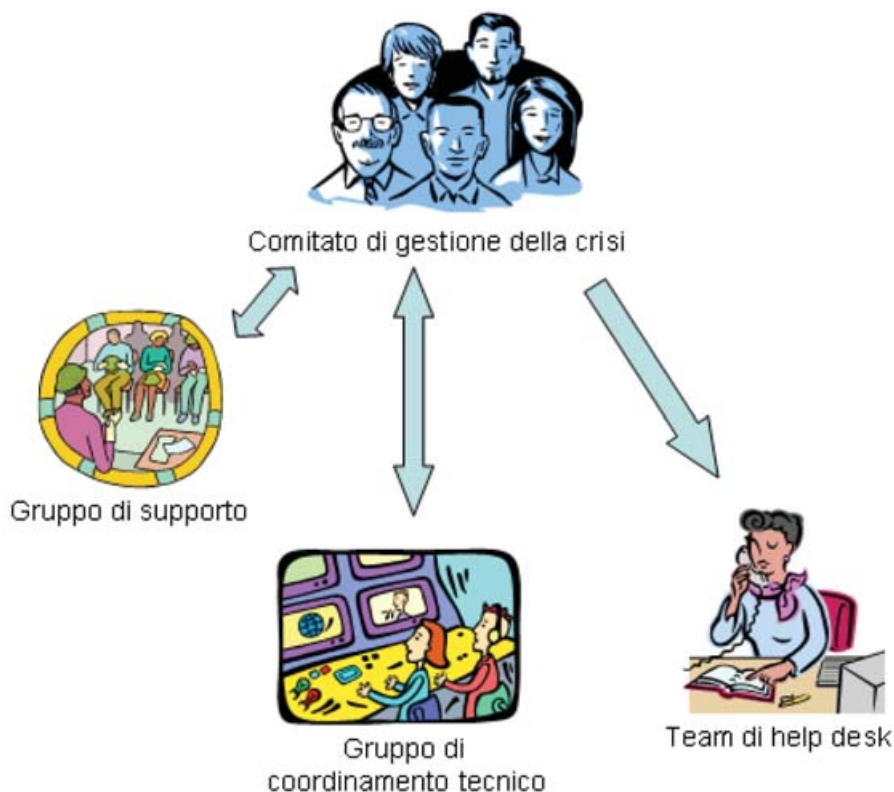
Figura 18

Ovviamente i nomi dei vari gruppi sono indicativi, ciò che conta sono le attività e le responsabilità a essi delegate, che sono diverse in condizioni ordinarie e in condizioni di emergenza. Tali attività e responsabilità sono descritte nei paragrafi seguenti.

3.4.1 Funzioni del Comitato di gestione della crisi

Il Comitato di gestione della crisi è un organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività degli altri gruppi. È l'organo di direzione strategica dell'intera struttura, e ha inoltre responsabilità di garanzia e controllo sull'intero progetto.
I suoi compiti principali sono:

- approvazione del piano di continuità operativa;
- valutazione delle situazioni di emergenza e dichiarazione dello stato di crisi;
- avvio delle attività di recupero e controllo del loro svolgimento;
- rapporti con l'esterno e comunicazioni ai dipendenti;

- attivazione del processo di rientro[44];
- avvio delle attività di rientro alle condizioni normali e controllo del loro svolgimento;
- dichiarazione di rientro;
- gestione di tutte le situazioni non contemplate;
- gestione dei rapporti interni e risoluzione dei conflitti di competenza[45];
- promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità.

In condizioni ordinarie il Comitato si riunisce con periodicità almeno annuale, allo scopo di valutare lo stato del progetto di continuità, verificare le criticità, attuare e pianificare le iniziative per il miglioramento continuo del progetto stesso.
In condizioni di emergenza, il Comitato assume il controllo di tutte le operazioni e assume le responsabilità sulle decisioni per affrontare l'emergenza, ridurne l'impatto e soprattutto ripristinare le condizioni preesistenti.
Per svolgere i propri compiti, il Comitato attiva le altre sottostrutture, e in particolare il Gruppo di supporto, che fa in modo che il Comitato possa disporre di strumenti e competenze per affrontare ogni sua decisione.
Il Comitato deve essere supportato nelle seguenti aree:

- **area logistica**, garantendo supporto per gli spostamenti, gli alloggi, ecc.;
- **area tecnologica**, al fine di garantire il funzionamento e l'accesso a tutte le infrastrutture informatiche e di telecomunicazioni predisposte;
- **area informazioni**, tramite aggiornamento di tutte le notizie provenienti dai canali pubblici di comunicazione;
- **area comunicazioni di processo**, tramite raccolta di tutti i rapporti di stato dai vari gruppi di lavoro.

Può essere necessario assicurare al Comitato un supporto di consulenza anche sulle aree:

- **comunicazioni**, ad esempio tramite valutazione delle strategie di comunicazione verso cittadini, organizzazioni e dipendenti e dei canali da utilizzare per ciascun tipo di comunicato;
- **finanza**, ad esempio con definizione di tutte le iniziative di carattere finanziario necessarie ad assicurare risorse tempestive;
- **risorse umane e rapporti sindacali**, ad esempio definizione di comportamenti e formulazione di messaggi specifici volti a rassicurare i dipendenti, sensibilizzare

[44] Il processo di rientro deve essere attuato dagli specifici gruppi operativi, ma deve essere continuamente monitorato dal Comitato, per assicurare la verifica dello stato di avanzamento complessivo e risolvere i casi dubbi. Infatti, per loro natura le operazioni di rientro, per quanto dettagliate, possono presentare imprevisti o azioni che coinvolgono altre persone e hanno impatto su molteplici attività. In tutti questi casi il Comitato deve acquisire tutti gli elementi utili a condurre alla soluzione del problema.

[45] La gestione dei rapporti interni è di primaria importanza: in situazione d'emergenza, caratterizzata da incertezze, difficoltà di comunicazione, stress, nervosismo e stanchezza, il personale si trova a operare nelle peggiori condizioni, quando invece è indispensabile il massimo contributo. È necessario pianificare un'attenta, precisa ed essenziale informazione per consentire a tutti di lavorare con efficacia e serenità.

quelli coinvolti nelle operazioni di ripristino, dirimere ogni possibile motivo di disagio che possa ridurre l'efficacia dell'organizzazione;

- **sicurezza informatica**, con l'esame di tutti gli aspetti di sicurezza, in particolare per quanto riguarda la verifica del grado di sicurezza offerto dalle configurazioni adottate per l'emergenza e la protezione dei dati, o tramite il riesame delle soluzioni adottate per il ripristino dei sistemi e per il rientro alla normalità.

3.4.2 Funzioni del Gruppo di supporto

Il Gruppo di supporto è una struttura amministrativa che fornisce supporto al Comitato di gestione della crisi, ed è responsabile – nella gestione ordinaria – delle seguenti funzioni:

- redazione del piano di continuità operativa;
- gestione e manutenzione del piano di continuità operativa (compreso l'aggiornamento dei riferimenti interni del personale);
- adeguamento periodico dell'analisi di impatto (BIA);
- studio di scenari di emergenza e definizione delle strategie di rientro;
- gestione dei rapporti con le assicurazioni;
- attuazione delle attività di divulgazione e di sensibilizzazione interna sui temi della continuità.

Dovendo offrire supporto su più temi, questo Gruppo dovrà essere costituito da esperti di gestione del patrimonio tecnologico, di risorse umane, di formazione, di logistica, di supporto amministrativo, di rapporti con i fornitori.
Il Gruppo di supporto si identifica (almeno per le pubbliche amministrazioni centrali) con il Comitato della sicurezza ICT della Direttiva del 16 gennaio 2002 del DIT. Nelle realtà con estensione territoriale è necessaria anche un'organizzazione periferica.
In condizioni di emergenza, il Gruppo di supporto è responsabile del coordinamento gestionale delle attività e di relazione sullo stato delle stesse al Comitato. Il Comitato e il Gruppo di supporto, in caso di necessità, si riuniscono presso un apposito sito di direzione delle operazioni.

3.4.3 Funzioni del Gruppo di coordinamento tecnico

Il Gruppo di coordinamento tecnico è responsabile di tutte le attività operative e tecniche connesse con l'esecuzione delle procedure di recupero e rientro. Nel dettaglio, in condizioni ordinarie tali attività sono:

- esercitazioni e test periodici;
- manutenzione dell'infrastruttura tecnologica e applicativa di recupero.

Mentre in condizioni di emergenza le attività sono:

- coordinamento del personale operativo in emergenza;
- organizzazione dei trasporti e della logistica del personale operativo in emergenza;
- notifica dello stato di avanzamento al Comitato di gestione della crisi;
- gestione del budget per spese straordinarie legate all'emergenza;

- monitoraggio del funzionamento delle applicazioni e dei sistemi in configurazione di ripristino;
- controllo e verifica dell'esito delle procedure di salvataggio e quadratura;
- interfaccia con gli outsourcer in condizioni di crisi.

È opportuno individuare formalmente i componenti di questo Gruppo. Esso in genere è costituito da:

- il responsabile dei sistemi informativi dell'amministrazione, che lo presiede;
- i responsabili delle unità organizzative tecniche, applicative e logistiche.

Il Gruppo di coordinamento tecnico potrebbe anche aver necessità di organizzare altri gruppi di persone a proprio supporto (tecnico, decisionale e organizzativo) che agiscano alle sue dipendenze per tutto il periodo d'emergenza. Ad esempio, potrebbe esserci la necessità di formare:

- un gruppo applicativo;
- un gruppo operativo;
- un gruppo di rientro.

Il gruppo applicativo è responsabile di tutte le attività sulle applicazioni e i dati ad esse associati. In particolare, a questo gruppo è assegnato il compito, in condizioni di emergenza, di:

- monitorare il funzionamento delle applicazioni e attivare eventuali interventi correttivi;
- sincronizzare le proprie attività con quelle del gruppo operativo e con quelle dell'help desk;
- controllare l'esito delle procedure di salvataggio;
- assicurare il funzionamento dell'infrastruttura applicativa nel sito alternativo.

Il gruppo operativo è responsabile di tutte le operazioni che coinvolgono i sistemi informatici e la rete di telecomunicazioni. In particolare, in condizioni di emergenza questo gruppo deve:

- monitorare il funzionamento dei sistemi;
- coordinare le attività con quelle del gruppo applicativo e con quello di help desk.

Il gruppo di rientro è responsabile di tutte le operazioni necessarie a garantire la ripresa della normale operatività presso il sito di esercizio. Per la natura delle attività da supportare e per l'estrema variabilità delle emergenze (e l'ampio numero degli scenari d'emergenza possibili), il compito del gruppo di rientro è da considerarsi molto gravoso.
Le attività di questo gruppo, in condizioni di emergenza, sono:

- rilevazione dei danni[46];
- gestione di tutte le operazioni di rientro;
- test dell'infrastruttura ripristinata nel sito di esercizio.

[46] La valutazione dei danni deve essere presentata al più presto al Comitato, e deve essere aggiornata frequentemente.

La comunicazione tra i diversi gruppi di lavoro descritti deve essere basata sul principio che chi è incaricato di eseguire una procedura:

- comunica alla persona o alla struttura superiore, a richiesta, lo stato in cui si trova;
- riceve notizia di tutte le decisioni che lo riguardano e dei riflessi di queste sulle procedure nelle quali è coinvolto.

3.4.4 Funzioni del team di help desk

In generale è opportuno definire un team di help desk specifico per la continuità operativa, i cui compiti sono:

- aggiornamento dei sistemi di gestione della conoscenza a supporto degli operatori del normale help desk (riguardo alle tematiche da affrontare in caso di emergenza);
- rafforzamento del normale help desk di primo livello in caso di emergenza;
- predisposizione di canali alternativi (al normale help desk) da adottare in caso di emergenza e diffusione presso gli utenti dei riferimenti relativi;
- fornitura di informazioni sullo stato dei sistemi in periferia al Gruppo di coordinamento tecnico;
- supporto agli utenti nelle difficoltà connesse alla ripresa delle attività al rientro.

Nella costituzione di tale team devono essere valutati specialmente la capacità di operare in assenza dei servizi informatici, la capacità di utilizzare canali multipli di comunicazione con gli utenti e la capacità di lavorare in situazione di emergenza.

3.5 Processi di formazione

I processi di formazione, informazione e sensibilizzazione da attuare con una logica top-down sono da sponsorizzare da parte dei massimi vertici dell'amministrazione, in quanto fattori importanti almeno quanto quelli tecnologici. Principali argomenti da trattare nell'ambito della formazione del personale addetto alle operazioni di mantenimento della continuità sono i seguenti:

- definizione di emergenza e di disastro;
- struttura organizzativa per l'emergenza;
- priorità decisionali e gestione dei rapporti interpersonali durante l'emergenza;
- canali di comunicazione e riferimenti informativi alternativi;
- procedure specifiche per settore;
- processo di rientro.

Per quanto riguarda gli utenti, il piano di formazione dovrà indirizzarne i comportamenti in caso di emergenza e l'uso di specifici strumenti quali i canali d'informazione d'emergenza e le procedure alternative per i servizi.
Per quanto attiene il processo di informazione e sensibilizzazione diffusa di tutto il personale, è da tener presente che la buona riuscita del Piano dipende da un gran numero di componenti dell'organizzazione.

Obiettivi essenziali del piano formativo sono:

- concetti di disastro;
- organizzazione, ruoli e limiti di azione durante le emergenze;
- linee guida di comportamento.

I contenuti della sensibilizzazione devono comprendere almeno i seguenti temi:

- processi di comunicazione in situazione di emergenza;
- utilizzo di strategie di comunicazione alternative;
- procedure di ripristino.

Si sottolinea anche l'importanza delle sessioni di simulazione, specialmente di quelle (concettuali) destinate ai vertici dell'amministrazione, in particolare al Comitato di gestione della crisi, il quale dovrà sottoporsi a sedute periodiche in cui verificare e affinare la capacità di valutare gli imprevisti e di reagire alle situazioni di emergenza.

3.6 CRITERI E INDICAZIONI ORGANIZZATIVE

In generale, nell'ambito delle problematiche legate alla creazione e gestione di una soluzione di continuità, una particolare attenzione deve essere riservata al coinvolgimento del personale interno, soprattutto nei casi in cui la gestione delle infrastrutture informatiche sia di competenza, in tutto o in parte, di personale interno all'amministrazione e non affidata in outsourcing a società esterne.
Si richiama la necessità assoluta di predisporre e aggiornare periodicamente elenchi di riferimenti per tutte le persone coinvolte nelle attività di gestione dell'emergenza e ripristino, individuando chiaramente e controllando chi è tenuto a effettuare queste attività. Ovviamente tali elenchi hanno elevato carattere di riservatezza, contenendo anche informazioni personali.
Allo scopo di non instaurare un clima di conflittualità sia nelle fasi di avvio e sviluppo del progetto sia, a maggior ragione, nelle fasi ben più importanti di esercizio a regime, è opportuno stabilire alcuni principi fondamentali sia nei confronti del personale interno, sia nei confronti del fornitore. Tali principi vengono espressi nei paragrafi seguenti.

3.6.1 INDICAZIONI PER L'AVVIO DEL PROGETTO

Nella fase di avvio del progetto occorre coinvolgere sin dall'inizio il personale addetto alla gestione delle infrastrutture, chiarendo nel modo più dettagliato possibile la ripartizione dei compiti tra fornitore e amministrazione.
Occorre inoltre che il personale dell'amministrazione si senta protagonista dell'intera operazione. Quindi, i dirigenti debbono illustrare le motivazioni, non solo tecniche, che sono alla base della soluzione scelta.
Nella fase di avvio occorre infine sensibilizzare anche le funzioni esterne all'area informatica (organizzazione, gestione del personale, organi tecnici quali ingegneri e avvocati, ecc.) in quanto tali funzioni saranno interessate alla stesura e all'approvazione del Piano che costituirà il documento essenziale per la corretta gestione della continuità.

3.6.2 Indicazioni per la realizzazione del progetto

Nelle fasi realizzative del progetto, pur nella necessaria ripartizione delle responsabilità tra amministrazione e fornitore, occorre dedicare la massima attenzione a che il personale interno non si senta escluso dalle scelte tecniche e organizzative che via via saranno attuate.
È vero che tali scelte dovrebbero essere previste nel capitolato di gara, ma trattandosi di un progetto di notevole complessità non si può escludere l'eventualità di cambiamenti "in itinere" che dovranno essere sempre condivisi e illustrati con la massima trasparenza.
Ad esempio, è opportuno stabilire un colloquio permanente tra il personale del sito primario e il personale del sito alternativo, in modo tale che ogni decisione sia concordata e condivisa.

3.6.3 Indicazioni per il collaudo

Il collaudo deve essere effettuato dal personale dell'amministrazione, sulla base delle specifiche predisposte dal fornitore, e in contraddittorio con il personale del fornitore stesso, cercando di riprodurre nel modo più dettagliato possibile il verificarsi di un'emergenza reale.

3.6.4 Indicazioni per il piano di continuità operativa

In fase di stesura del Piano occorre risolvere tutte le problematiche relative all'impegno di personale interno all'amministrazione, con riferimento non solo al personale tecnico IT, ma a tutte le funzioni aziendali coinvolte nell'erogazione dei servizi critici, ivi compreso il personale addetto alla gestione delle applicazioni e al contatto con gli utenti delle stesse.
L'emergenza potrebbe infatti modificare in tutto o in parte gli abituali aspetti organizzativi e logistici, con la conseguente necessità di operare in modalità completamente diverse da quella ordinaria.
Potrebbe ad esempio essere necessario cambiare la sede di lavoro, utilizzare procedure diverse per la gestione delle applicazioni, informare gli utenti esterni ed interni sull'impossibilità di fornire alcuni servizi o fornirli comunque in maniera ridotta.
Occorre quindi concordare con le organizzazioni sindacali tutte le procedure straordinarie che rendano possibile la continuità dei servizi critici. Ad esempio occorre:

- definire dettagliatamente ruoli e responsabilità di tutti gli attori;
- concordare la possibilità di convocare il personale in qualunque orario;
- definire un budget idoneo al pagamento di competenze accessorie quali turni e straordinario e definire altresì le modalità amministrative con le quali disporre di tali somme con rapidità;
- definire la possibilità di utilizzare mezzi di trasporto privati (ad es. taxi);
- definire la possibilità di convocazioni in missione;
- concordare le procedure alternative con le quali erogare i servizi essenziali.

È indispensabile, infine, che tutto quanto concordato ai punti precedenti sia inserito in un documento ufficiale approvato ai massimi livelli dell'amministrazione, e che tale documento sia continuamente aggiornato e reso disponibile a quanti dovranno gestire l'emergenza.

3.6.5 Indicazioni per la gestione e la manutenzione

È buona pratica che tutte le operazioni amministrative legate alla gestione della soluzione di continuità (ad esempio le convocazioni di riunioni, la creazione di liste di distribuzione, l'aggiornamento della documentazione on line e cartacea, ecc.) siano di competenza di una "segreteria del progetto di continuità".
Dal punto di vista organizzativo, la gestione della soluzione di continuità prevede una serie di riunioni ordinarie e di riunioni straordinarie dei vari gruppi di lavoro coinvolti. Ad esempio, è necessario indire delle periodiche riunioni ordinarie del Gruppo di supporto, con lo scopo di:

- verificare la rispondenza del Piano alle esigenze dell'amministrazione;
- pianificare i test del Piano;
- verificare la validità dei test stessi a prove ultimate.

È opportuno che le riunioni ordinarie abbiano una frequenza semestrale, e precedano il periodo previsto per i test, in modo da consentirne una corretta e precisa pianificazione. Inoltre possono essere riconvocate dopo i test, qualora questi non abbiano avuto esito positivo.
Si suggerisce che la segreteria del progetto di continuità invii la convocazione delle riunioni ordinarie ai componenti del Gruppo e, per conoscenza, al sostituto di ogni componente, attraverso il mezzo più idoneo (fax, e-mail, ecc.), con almeno 15 giorni di preavviso. L'oggetto della comunicazione deve contenere in evidenza la dicitura "Continuità operativa – riunione ordinaria". La convocazione deve contenere anche l'ordine del giorno previsto per la riunione, che dovrà comunque sempre prevedere almeno i seguenti due punti:

- check-list di verifica dell'aggiornamento del Piano;
- pianificazione dei test.

Ciascun componente del Gruppo deve confermare alla segreteria del progetto la partecipazione alla riunione con almeno una settimana di anticipo sulla data della riunione. In caso di mancata conferma nei tempi previsti, la segreteria provvederà a convocare il sostituto.
Nel corso delle riunioni ordinarie avviene anche la pianificazione dei test, e viene anche fissata la durata degli stessi, che è diversa a seconda della tipologia di test scelta e delle caratteristiche della soluzione di continuità da verificare (la durata può andare da alcune ore a qualche giorno lavorativo).
Al termine del test deve essere compilato un dettagliato verbale per certificarne l'esito. In caso di insuccesso parziale o totale dei test, il Gruppo di supporto deve esaminare le problematiche emerse e attivare le azioni necessarie per la loro risoluzione.
È compito del Gruppo ridigere il resoconto della riunione ordinaria, che deve sempre contenere:

- le non conformità evidenziate dalla valutazione della check-list di manutenzione ordinaria del Piano, con relative azioni da intraprendere per la loro rimozione, persona o struttura incaricata e scadenza prevista;
- il verbale dei risultati dei test in allegato;

- le azioni da intraprendere per la rimozione degli eventuali problemi riscontrati nel corso dei test unitamente alla persona o struttura incaricata di rimuoverli e alla scadenza prevista.

Copia del resoconto della riunione ordinaria deve essere distribuita a:

- tutti i componenti del Comitato di gestione;
- tutti i componenti del Gruppo di supporto;
- ai responsabili delle squadre degli addetti alla gestione operativa.

È compito del responsabile del Gruppo verificare che le non conformità evidenziate dalla valutazione della check-list e i problemi evidenziati nei test di manutenzione ordinaria siano rimossi nei tempi previsti. I verbali delle riunioni di manutenzione ordinaria devono essere archiviati in formato magnetico e cartaceo presso la segreteria di progetto.
La riunione straordinaria, viceversa, è il meccanismo attraverso il quale il Comitato di gestione e il Gruppo di supporto recepiscono i cambiamenti organizzativi dell'amministrazione, i cambiamenti tecnici del sistema informativo e di quant'altro possa esercitare un impatto sostanziale sulla struttura e/o sul contenuto del Piano.
Le riunioni straordinarie, a causa della loro tipologia, non possono avere una frequenza prestabilita. La loro convocazione, in caso di necessità, è demandata al responsabile del Gruppo di supporto.
La segreteria del progetto invia la convocazione della riunione straordinaria ai componenti del Comitato di gestione e del Gruppo di supporto e, per conoscenza, ai sostituti di ogni componente, attraverso il mezzo più idoneo (fax, e-mail, ecc.), con preavviso minimo. L'oggetto della comunicazione deve contenere in evidenza la dicitura "Continuità operativa – riunione straordinaria".
Ciascun componente del Gruppo deve confermare la partecipazione alla riunione alla segreteria del progetto. In caso di mancata conferma nei tempi previsti, la segreteria provvederà a convocare il sostituto.

3.6.6 Indicazioni per la documentazione

Come già detto precedentemente, per assicurarsi che la soluzione di continuità sia perfettamente funzionante in caso di necessità, è fondamentale che la documentazione sia disponibile in ogni momento, sia mantenuta sempre aggiornata e che le versioni successive dei manuali vengano distribuite in modo corretto agli interessati.
Ogni modifica a uno qualsiasi dei documenti che costituiscono il Piano, siano essi manuali o allegati esterni, ne comporterà una variazione di modifica e/o release.
Una modifica a un manuale o a un allegato esterno che scaturisca da una manutenzione ordinaria darà luogo a una nuova release del documento (passerà da m.n a m.n+1). Una modifica a un manuale o a un allegato esterno che scaturisca da una manutenzione straordinaria darà luogo a una nuova versione del documento (passerà da m.n a m+1.0). Dovranno essere aggiornati di conseguenza i dati di controllo presenti nella copertina del documento, la versione nel pié di pagina e la data nell'intestazione.
A ogni nuova versione o release di uno dei documenti che costituiscono il Piano sarà creata una nuova versione o release dell'allegato esterno "Indice dei documenti" contenente gli estremi delle ultime versioni o release modificate.

La copia cartacea delle nuove versioni o release dovrà essere firmata per approvazione sulla copertina dal responsabile del Gruppo di supporto unitamente alla data di approvazione. Dopo la firma, la segreteria del progetto di continuità aggiornerà la copia magnetica inserendo il nome del responsabile del Gruppo di supporto e la data di approvazione, e archivierà il documento in formato magnetico e in formato cartaceo secondo lo standard della segreteria.
La segreteria del progetto, a ogni nuova versione/release dei documenti che costituiscono il Piano, ha il compito di curare la distribuzione dello stesso affinché le "copie ufficiali" del Piano siano sempre aggiornate.

4. Strumenti giuridici e operativi per l'acquisizione di un servizio di continuità

4.1 Considerazioni generali

Seguendo i metodi esaminati nei capitoli precedenti e sulla base di considerazioni di natura organizzativa, tecnica ed economica, le amministrazioni, una volta definita la soluzione di continuità operativa più adeguata alla proprie caratteristiche, procedono alla sua realizzazione attraverso l'acquisizione delle necessarie infrastrutture e servizi.
Anche le amministrazioni che scelgono una soluzione organizzata e gestita, in tutto o in parte, internamente, dovranno acquisire le infrastrutture necessarie (si veda in proposito quanto indicato nell'allegato tecnologico alle presenti linee guida). In generale, sarà necessario acquisire non solo apparati e software ma, anche, locali, presumibilmente già attrezzati o da attrezzare, servizi di comunicazione, ecc.
Tutti gli elementi presentati e discussi nei tre precedenti capitoli hanno messo in evidenza quanto, in tema di servizi di continuità operativa, sia vasto, complesso e di non facile gestione l'insieme delle attività e degli aspetti concernenti l'acquisizione delle forniture e i costi.
Inoltre, le stesse considerazioni sulla complessità delle attività in questione possono rendere conveniente e favorire l'associazione di più amministrazioni nel processo di acquisizione e fruizione dei servizi, essendo, quella condivisa, la modalità che migliora, riducendolo, il rapporto tra costi e benefici. Va anche detto che l'associazione di più amministrazioni può anche essere realizzata senza alcuna fornitura esterna e, anzi, utilizzando, esclusivamente o in parte, solo le infrastrutture esistenti presso le amministrazioni associate. Tale modalità, già discussa sotto il profilo metodologico, è quella del "mutuo soccorso".
In questo capitolo sono presentati gli elementi normativi di riferimento per la continuità operativa, con particolare riguardo a quelli da considerare nel caso che questi servizi vengano acquisiti da fornitore esterno.
Sono poi esaminate le forme di collaborazione possibili tra amministrazioni centrali e quelle previste per le Regioni e gli Enti locali.
Il capitolo comprende l'illustrazione di un esempio di tre atti – protocollo d'intesa, contratto e capitolato tecnico – per l'acquisizione di servizi di continuità operativa da parte di pubbliche amministrazioni. In allegato sono forniti i testi esemplificativi degli atti in esame.
Infine, data la particolarità del caso di amministrazioni che si accordino per la modalità di servizi in "mutuo soccorso", caso che si ritiene di interesse soprattutto per amministrazioni medio-piccole, in chiusura del capitolo è riportato un esempio del percorso contrattuale che è possibile seguire per questa ipotesi.

Nel presente capitolo vengono forniti:

- una panoramica delle norme in materia di continuità operativa;
- un quadro delle principali norme che disciplinano le procedure di acquisizione di beni e servizi.

4.2 Norme in materia di continuità operativa

Direttiva del 16 genaio 2002

La Direttiva recante "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali", del 16 gennaio 2002, pubblicata sulla G.U. n. 69 del 22 marzo 2002 sollecita le pubbliche amministrazioni a porre attenzione ai temi della sicurezza, valutando i rischi e attuando contromisure in grado di contenerne probabilità e conseguenze. Di seguito si riportano alcuni stralci della direttiva a testimonianza di quale attenzione deve essere posta sul tema in questione:

> *"Sicurezza nelle tecnologie dell'informazione e della comunicazione*
>
> *Le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese. Questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse. È noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e di distruzione del servizio.*
>
> *Lo stesso processo di innovazione tecnologica produce da un lato strumenti più sofisticati di "attacco", ma d'altro lato idonei strumenti di difesa e protezione. Assume quindi importanza fondamentale valutare il rischio connesso con la gestione delle informazioni e dei sistemi. Inoltre per poter operare in un mondo digitale sempre più aperto, le pubbliche amministrazioni devono essere in grado di presentare credenziali di sicurezza nelle informazioni conformi agli standard internazionali di riferimento.*
>
> *...*
>
> *Data l'importanza ed attualità del tema in oggetto e nella consapevolezza del grande impegno richiesto in termini di competenze e risorse da mobilitare si raccomanda a tutte le pubbliche amministrazioni di agire con la massima priorità ed urgenza per quanto riguarda le azioni immediate preventivamente descritte.*
>
> *...."*

Alla citata Direttiva è allegato un documento, al quale si rimanda, che illustra le misure di base che le amministrazioni pubbliche devono attuare nel breve periodo.

Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196)

Anche la normativa in materia di trattamento dei dati personali deve essere presa in considerazione nel disegnare soluzioni di continuità operativa: la legge infatti mira a tutelare l'integrità, la disponibilità e la riservatezza dei dati, stabilendone le modalità di trattamento. I primi due aspetti (integrità e disponibilità) costituiscono l'obiettivo principale delle soluzioni di continuità operativa.

I rischi di distruzione e perdita sono citati nell'articolo 31 (Obblighi di sicurezza):

> "*I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*"

Nell'articolo 34 (Trattamento con strumenti elettronici) si fa riferimento alle misure minime di sicurezza da adottare:

> "…
>
> *f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;"*

Codice dell'amministrazione digitale (Decreto legislativo 7 marzo 2005, n. 82)

Il Codice dell'amministrazione digitale richiama la necessità di salvaguardare i dati attinenti servizi pubblici. Il Codice richiede, tra l'altro, una particolare attenzione da parte delle amministrazioni alla custodia dei dati, in modo da garantire il diritto dei cittadini e delle imprese a "*richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali*" (Art. 3 – Diritto all'uso delle tecnologie).
Va anche tenuta presente la necessità di garantire riscontri delle transazioni finanziarie riguardanti pagamenti verso la PA centrale, come previsto dall'art. 5 (Effettuazione dei pagamenti con modalità informatiche):

> "*A decorrere dal 30 giugno 2007, le pubbliche amministrazioni centrali con sede nel territorio italiano consentono l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, con l'uso delle tecnologie dell'informazione e della comunicazione.*"

Più in particolare, il principio della custodia e salvaguardia dei dati è fissato all'art. 51 (Sicurezza dei dati), comma 2:

> "*I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.*"

È anche affermato il diritto del cittadino ad avere a disposizione modulistica in formato elettronico, come previsto all'art. 57 (Moduli e formulari) che ribadisce il principio di assicurare la massima affidabilità della custodia documentale:

> "*1. Le pubbliche amministrazioni provvedono a definire e a rendere disponibili anche per via telematica l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.*
>
> *2. Trascorsi ventiquattro mesi dalla data di entrata in vigore del presente codice, i moduli o i formulari che non siano stati pubblicati sul sito non possono essere richiesti ed i relativi procedimenti possono essere conclusi anche in assenza dei suddetti moduli o formulari*".

DPCM 31 maggio 2005 (Gazz. Uff. 18 giugno 2005, n. 140)
Questo Decreto rappresenta un provvedimento fondamentale per la continuità operativa delle pubbliche amministrazioni, in quanto prevede direttamente che le pubbliche amministrazioni di cui al D.Lgs. 39/93 assumano iniziative volte ad assicurare la continuità operativa. In questo contesto, il CNIPA svolge un ruolo di indirizzo e coordinamento anche, per esempio, attraverso le presenti linee guida.
In particolare, all'art. 3, lettera c) di tale Decreto, recante "*Razionalizzazione in merito all'uso delle applicazioni informatiche e servizi ex articolo 1, commi 192, 193 e 194 della legge n. 311 del 2004 (Finanziaria 2005)*", stabilisce che "*Gli obiettivi di miglioramento dell'efficienza operativa della pubblica amministrazione e di contenimento della spesa pubblica sono conseguiti mediante interventi di razionalizzazione di infrastrutture di calcolo, telematiche e di comunicazioni delle amministrazioni di cui all'art. 1 del decreto legislativo 12 febbraio 1993, n. 39, anche con l'introduzione di nuove tecnologie e servizi.*
Gli interventi riguardano:

> *...*
> *c) centri per garantire la salvaguardia dei dati e delle applicazioni informatiche e la continuità operativa dei servizi informatici e telematici, anche in caso di disastri e di situazioni di emergenza, attraverso la definizione di infrastrutture, sistemi e servizi comuni a più amministrazioni, anche utilizzando CED già esistenti.*".
> *Il CNIPA, ai fini di cui al comma 1, svolge funzioni di impulso e coordinamento, anche attraverso l'indizione di conferenze di servizi.".*

DPCM 6 agosto 1997, n. 452 (Gazz. Uff. 30 dicembre 1997, n. 302)
Non va omesso di menzionare tale decreto contenente "*Regolamento recante approvazione del capitolato di cui all'articolo 12, comma 1, del D.Lgs. 12 febbraio 1993, n. 39, relativo alla locazione e all'acquisto di apparecchiature informatiche, nonché alla licenza d'uso dei programmi*", il quale, ancorché non direttamente correlato al tema della continuità operativa, riveste comunque la massima importanza anche per la materia trattata dalle presenti Linee guida in quanto l'art. 3 del medesimo, dopo aver rammentato che la redazione dello studio di fattibilità precede tutti i contratti di grande rilievo ai sensi dell'articolo 9 e dell'articolo 17, comma 2, del decreto legislativo 12 febbraio 1993, n. 39, ne definisce gli obiettivi ed i contenuti.
Conseguentemente, la disciplina recata dal citato articolo troverà applicazione anche per la redazione dello studio di fattibilità che precederà la fase di progettazione dell'iniziativa che qui ci occupa, ancorché la stessa non sia definibile di grande rilievo.

* * *

Non va infine dimenticato il documento "*Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione*" del Comitato Tecnico Nazionale di sicurezza informatica del marzo 2004, la cui seconda parte, "Linee guida per l'attuazione della sicurezza ICT nella PA", contiene l'indicazione di una serie di attività, che il Comitato ritiene di estrema urgenza, per l'analisi del rischio e la continuità operativa.

4.2.1 Normativa generale per l'acquisizione di beni e servizi

Il conferimento da parte di una pubblica amministrazione, ad un apposito soggetto, dell'incarico di erogare i servizi e fornire i beni necessari ad assicurare all'amministrazione

medesima la continuità operativa, dovrà essere preceduto dallo svolgimento della procedura di selezione del contraente.
La principale normativa comunitaria e nazionale di riferimento è:

- la Direttiva 31 marzo 2004, n. 2004/18/CE, recante "Direttiva del Parlamento europeo e del Consiglio relativa al coordinamento delle procedure di aggiudicazione degli appalti pubblici di lavori, di forniture e di servizi";
- il decreto legislativo 12 aprile 2006, n. 163, recante "Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE".

4.2.2 Forme di collaborazione tra pubbliche amministrazioni centrali

Premesso che per tali amministrazioni risulta – in via generale – non attuabile alcuna soluzione che preveda l'erogazione di beni e servizi dalle stesse a favore di altre pubbliche amministrazioni, si sottolinea che alla luce di quanto disposto dall'ordinamento, l'unica forma di collaborazione tra amministrazioni centrali per la gestione in comune di un centro di continuità operativa appare lo strumento previsto dall'art. 15 della legge 7 agosto 1990, n. 241 il quale prescrive:

> "*Anche al di fuori delle ipotesi previste dall'articolo 14, le amministrazioni pubbliche possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune.*
> *Per detti accordi si osservano, in quanto applicabili, le disposizioni previste dall'articolo 11, commi 2, 3 e 5.*".

Secondo quanto ritenuto dalla Corte dei conti, "*Le convenzioni fra amministrazioni pubbliche di cui all'art. 15 della legge n. 241 del 1990 costituiscono lo strumento per disciplinare lo svolgimento in collaborazione di attività di interesse comune e, pertanto, per comporre in un quadro unitario gli interessi pubblici di cui ciascuna amministrazione è portatrice.*"[47].

Nel caso di specie, l'oggetto dell'accordo di cui al citato art. 15 potrà consistere in un'intesa che disciplinerà, ad esempio:

- l'espletamento di una procedura di gara comune finalizzata alla individuazione del soggetto al quale le amministrazioni affideranno l'incarico di erogare il servizio di continuità operativa;
- la costituzione di un centro comune di continuità operativa attraverso la messa a fattore comune delle risorse di ciascuna di esse dedicate a tale servizio.

La norma in questione, nell'interpretazione che della stessa ha fornito il Consiglio di Stato, ben si presta per il conseguimento degli obiettivi di cui alle presenti Linee guida poiché, secondo il supremo Organo di giustizia amministrativa *"Ex art. 15 comma 1 l. 7 agosto 1990 n. 241, le amministrazioni pubbliche possono "sempre" concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune, le quali ben possono riguardare attività materiali da svolgere nell'espletamento di un pubblico servizio e direttamente in favore della collettività.*"[48].

[47] Sez. Giur. Reg. Puglia, sent. n. 244 del 21-03-2003.
[48] Consiglio Stato, sez. VI, 8 aprile 2002, n. 1902.

Stante il rinvio operato dall'articolo in esame ai commi 2, 3 e 5 dell'art. 22 l. cit.:

- gli accordi di cui al richiamato art. 15 debbono essere stipulati, a pena di nullità, per atto scritto, salvo che la legge disponga altrimenti. Ad essi si applicano, ove non diversamente previsto, i princìpi del codice civile in materia di obbligazioni e contratti in quanto compatibili;
- gli accordi sostitutivi di provvedimenti sono soggetti ai medesimi controlli previsti per questi ultimi;
- le controversie in materia di formazione, conclusione ed esecuzione degli accordi sono riservate alla giurisdizione esclusiva del giudice amministrativo.

Allo stato attuale, non sembra che le norme vigenti in materia permettano di individuare altri strumenti operativi (ad es. i consorzi) – come invece risulta possibile per altre tipologie di amministrazioni – attraverso i quali le amministrazioni centrali possano procedere congiuntamente alla creazione/gestione di un centro di continuità operativa.

4.3 FORME DI COLLABORAZIONE TRA REGIONI ED ENTI LOCALI

Le Regioni e gli Enti locali interessati a sviluppare soluzioni che implementino la continuità operativa dei servizi informatici è opportuno che verifichino la possibilità di associarsi con altre amministrazioni al fine di ottimizzare i costi (siano essi organizzativi che tecnologici) che inevitabilmente scaturiranno dall'introduzione delle soluzioni prescelte.
A tal fine le amministrazioni possono adottare una delle forme associative previste dagli articoli da 30 a 35 del D.Lgs. 267 del 2000, recante il Testo Unico degli Enti Locali (di seguito TUEL) per disciplinare i rapporti di collaborazione; le forme previste dal TUEL sono:

- la convenzione;
- il consorzio;
- l'unione di comuni;
- gli accordi di programma.

Tali forme associative sono state già adottate dalle amministrazioni che hanno partecipato ai progetti di e-government cofinanziati dal CNIPA e la gestione associata di servizi e/o funzioni rappresenta sicuramente uno degli elementi più importanti per conseguire gli obiettivi di e-government.
Ferma restando la libertà delle amministrazioni nell'adottare la forma giuridica ritenuta più idonea, si ritiene quale forma più consona all'obiettivo quella della *convenzione* mentre appare di difficile applicazione la forma dell'unione di comuni specie se realizzata esclusivamente per la gestione in forma associata di un sistema di continuità operativa.
Di seguito si riporta una breve descrizione delle forme associative rappresentate dall'istituto della convenzione, del consorzio e dell'accordo di programma, che lungi dal voler essere esaustiva, rappresenta una prima indicazione per le amministrazioni circa gli adempimenti ed i "passaggi" amministrativi che esse dovranno intraprendere per associarsi.

4.3.1 La convenzione

La prima forma associativa che il TUEL disciplina è quella attuabile a mezzo di convenzione (art. 30).
Questo strumento risulta essere, in assoluto, quello ritenuto più importante dal legislatore per lo svolgimento congiunto dell'azione amministrativa tra Enti locali e ciò si evince, sia dalla citazione di tale strumento in diverse sezioni del TUEL, sia dal fatto che lo stesso consente l'esercizio dell'attività di cui sopra senza determinare, per gli enti aderenti, la rinuncia alle proprie prerogative istituzionali.
Occorre previamente ricordare che sarà di competenza dell'organo consiliare (art. 42 lett. c, del TUEL) l'approvazione della delibera avente ad oggetto la convenzione (sia che essa abbia ad oggetto rapporti tra Enti locali sia che il rapporto sia tra l'Ente locale ed un'altra pubblica amministrazione) e che sarà di competenza del rappresentante legale dell'amministrazione sottoscrivere l'atto.
L'articolo 30 prevede che la stipula della convenzione debba avere quale fine lo svolgimento in modo coordinato di determinate funzioni e/o servizi escludendo, quindi implicitamente, la possibilità di sottoscrivere convenzioni per realizzare un'opera pubblica.
Rispetto al significato dell'aggettivo "determinate", è da intendersi che non sono consentite convenzioni che genericamente facciano riferimento a servizi o funzioni pubbliche locali, senza specificarne il contenuto e le modalità di espletamento od erogazione.
Analizzando gli elementi essenziali di una convenzione, il primo che essa deve contenere, oltre alla durata, è la specificazione dei "fini", che evidentemente non dovranno consistere nella ripetizione di quanto già rientra negli scopi istituzionali affidati dall'ordinamento all'amministrazione.
Altro elemento richiesto è l'indicazione delle forme di consultazione tra gli enti aderenti; ci si riferisce evidentemente alle modalità attraverso le quali gli enti si coordinano e controllano l'attuazione degli scopi perseguiti con la convenzione.
Sarà necessario altresì:

- procedere alla quantificazione degli apporti finanziari a carico di ciascun ente, fermo restando che tale apporto può consistere anche in spese interne (risorse umane) o utilizzo di strutture già in possesso dell'ente;
- indicare i reciproci obblighi e garanzie; gli enti possono adottare istituti prettamente civilistici quali la clausola penale, la condizione risolutiva o sospensiva ecc.

Oltre a tali requisiti essenziali, la convenzione può comunque presentare contenuti facoltativi secondo le finalità che gli enti intendono raggiungere.
Con riferimento agli scopi delle presenti Linee guida, si sottolinea che il comma 4 dell'art. 30 stabilisce che "*Le convenzioni di cui al presente articolo possono prevedere anche la costituzione di uffici comuni, che operano con personale distaccato dagli enti partecipanti, ai quali affidare l'esercizio delle funzioni pubbliche in luogo degli enti partecipanti all'accordo, ovvero la delega di funzioni da parte degli enti partecipanti all'accordo a favore di uno di essi, che opera in luogo e per conto degli enti deleganti*".
Vengono così individuati due particolari mezzi organizzativi per la migliore attuazione degli obblighi e dei contenuti della convenzione.

Nel primo caso è evidente come gli uffici comuni non possano essere considerati come organismi amministrativi muniti di autonomia; pertanto l'attività da essi svolta dovrà essere ricondotta e imputata in capo ai soggetti che li hanno costituiti.
Nel secondo caso, invece, il delegato agirà in nome e per conto dei soggetti deleganti i quali a loro volta dovranno rispondere dell'operato del delegato nei confronti dei terzi, salvo il diritto di rivalersi nei confronti del delegato medesimo.

4.3.2 I CONSORZI

La seconda forma associativa che il TUEL disciplina è quella del consorzio di cui all'art. 31. L'oggetto del consorzio può consistere, oltre che nella gestione in comune di servizi, nell'esercizio, sempre in comune, di funzioni. Possono partecipazione al consorzio, oltre ai Comuni ed alle Province, anche le comunità montane e le unioni di comuni.
L'art. 31 del TUEL sancisce due tipologie di consorzio: il consorzio-azienda istituito per la gestione dei servizi e il consorzio-ente amministrativo istituito per l'esercizio associato di funzioni; mentre per i consorzi-azienda trovano applicazione le norme proprie delle aziende speciali, per i consorzi-ente si applicherà quella degli Enti locali.
Viene inoltre prevista la distinzione tra consorzio facoltativo, che è quello voluto per libera decisione degli enti partecipanti, e consorzio obbligatorio, in caso di specifica legge dello Stato, nel caso in cui vi sia un rilevante interesse pubblico.
Rispetto alla configurazione di soggetto di diritto, è ritenuto da opinione dominante sussistere in capo al consorzio la personalità giuridica e ciò in virtù del combinato disposto degli articoli 31 e 114 del TUEL. Infatti l'articolo 31 stabilisce che "*Gli enti locali per la gestione associata di uno o più servizi e l'esercizio associato di funzioni possono costituire un consorzio secondo le norme previste per le aziende speciali di cui all'articolo 114 ...*", articolo che definisce tali enti come strumentali e soprattutto dotati di personalità giuridica; deve comunque essere fatto presente che la locuzione "*in quanto compatibili*", recata dal citato articolo 31, lascia aperta la porta anche a diversa interpretazione.
Si evidenzia comunque come l'articolo 31, nel definire i tratti salienti della convenzione, finalizzata e strumentale alla costituzione del consorzio e definente lo statuto del medesimo – assimilabile quindi ad una sorta di patto paraconsortile – ne preveda puntualmente i contenuti essenziali che recano sicuri elementi rappresentativi di una soggettività giuridica. Infatti la convenzione deve disciplinare la rappresentanza degli interessi consortili in seno al nuovo organismo, con riguardo alle nomine ed alle competenze, affinché essi vengano gestiti in modo autonomo e deve inoltre prefigurare lo statuto del nuovo ente per la disciplina della sua organizzazione, nonché la nomina e la definizione delle funzioni attribuite agli organi consortili.
In tal senso, quindi, la norma individua un nuovo ente autonomo rispetto agli enti convenzionati, attribuendo al primo poteri di curare e gestire in modo autonomo i propri interessi con diretta imputazione di responsabilità anche nei confronti degli enti consorziati.
Il consorzio facoltativo è regolamentato in parte dalla legge, in parte dalla libera determinazione degli enti interessati.
Al fine di costituire un consorzio occorre che il competente organo dell'ente (il consiglio comunale o provinciale oppure l'assemblea nel caso di unione di comuni o comunità montane) deliberi a maggioranza assoluta dei componenti, compreso il Sindaco o il Presidente della Provincia.

Oggetto della deliberazione è la convenzione e lo statuto del consorzio, entrambi, necessariamente, da approvarsi nella medesima seduta.
La convenzione, in questo caso, nulla ha a che vedere con la convenzione di cui all'art. 30, essendo quest'ultima direttamente finalizzata a gestire il coordinamento tra gli enti mentre, nel caso di specie, è, come detto, strumentale alla costituzione di altra e diversa forma organizzativa, quella consortile.
Nello statuto deve essere regolamentata l'organizzazione, la nomina e le funzioni degli organi consortili, mentre nella convenzione devono essere disciplinate:

- le nomine e le competenze degli organi consortili;
- le modalità di trasmissione agli enti consortili degli atti fondamentali del consorzio;
- le forme di consultazione, i rapporti finanziari, gli obblighi e le garanzie reciproche degli enti.

Non è consentito al consorzio avvalersi di propria azienda per la gestione del servizio rientrante nell'oggetto statutario o delegarlo a terzi ed esula altresì dalla potestà del consorzio la costituzione di nuove entità soggettive nella forma della S.p.A., tra soggetti pubblici e privati.
Gli organi previsti per il consorzio sono l'assemblea e il consiglio di amministrazione.
L'assemblea è composta dai Sindaci o dai Presidenti della Provincia o loro delegati o dagli altri legali rappresentanti degli altri enti; i membri partecipano all'assemblea con responsabilità pari alla quota di partecipazione fissata dalla convenzione e nello statuto.
L'assemblea, di regola presieduta da un componente dello stesso organo collegiale, è un organo a carattere permanente di durata coincidente con quella del consorzio, non soggetto a rinnovi per scadenze temporali; l'assemblea ha quali funzioni quella di determinare gli indirizzi, approvare gli atti fondamentali, esercitare la vigilanza e verificare i risultati conseguiti; la stessa, inoltre, elegge il consiglio di amministrazione.
Il consiglio di amministrazione, come appena ricordato, è eletto dall'assemblea nel numero di componenti e con le modalità previsti nella convenzione ed ha funzioni esecutive e decisionali rispetto alle attività del consorzio.
Altri organi del consorzio sono: il presidente del consiglio di amministrazione, il direttore, in quanto responsabile della gestione del consorzio e della direzione del personale, il segretario.
Come detto, oggetto della gestione consortile può essere, oltre ai servizi pubblici compresi quelli sociali, anche l'esercizio in comune di funzioni, elemento, questo, che comporta la variazione della disciplina applicabile.
Rispetto al rapporto tra le forme associative previste dall'art. 30 e dall'art. 31 del TUEL, si può ritenere che, ove si tratti solo di coordinare servizi e funzioni, agli Enti locali converrà adottare il mezzo più immediato della convenzione sottoposta a durata. Ove invece si avverta l'esigenza di un risultato cui necessiti, ad esempio, un servizio a rilevanza imprenditoriale oppure l'esercizio di una funzione organizzata, l'Ente locale, invece di costituire un'azienda speciale, potrà costituire un consorzio.
L'articolo 31, comma 7, infine, come già visto, prescrive che in caso di rilevante interesse pubblico, la legge possa prevedere la costituzione di consorzi obbligatori per l'esercizio di determinate funzioni e servizi la cui attuazione viene comunque demandata all'iniziativa della Regione.

4.3.3 Gli accordi di programma

Lo strumento in esame mira a "*ricondurre ad unità di intenti e di risultati l'azione pubblica finalizzata all'attuazione di interventi di particolare rilevanza, attraverso l'impiego di uno strumento tecnico di natura organizzatoria improntato al criterio dell'autocoordinamento spontaneo*".
L'oggetto dell'accordo di programma è esplicitato dall'art. 34 che avverte come tale strumento riguardi "*la definizione e l'attuazione di opere, di interventi o di programmi di intervento che richiedono, per la loro completa realizzazione, l'azione integrata e coordinata di comuni, di province e regioni, di amministrazioni statali e di altri enti pubblici; scopo dell'accordo è il coordinamento delle azioni e la determinazione dei tempi, le modalità, il finanziamento ed ogni altro connesso adempimento*".
I soggetti pertanto legittimati appaiono essere Regioni, Province e Comuni nonché amministrazioni locali e altri soggetti pubblici, mentre l'oggetto potrà essere la definizione e l'attuazione di opere, interventi o programmi di intervento, escludendosi quindi la realizzazione di servizi. Deve pertanto essere tenuto ben presente che l'utilizzo di tale strumento sarà in grado di realizzare solo alcuni degli obiettivi – tra l'altro eventuali – legati ad una soluzione di continuità operativa.
Per quanto riguarda i settori di intervento dell'accordo, non sembrano sussistere limitazioni al riguardo, ben potendosi verificare il caso di accordi relativi ad una singola opera pubblica ovvero a programmi di intervento a loro volta non necessariamente attuativi di precedenti atti di programmazione.
L'attività di impulso rispetto alla conclusione dell'accordo dovrà essere svolta dal Presidente della Regione o della Provincia o dal Sindaco in relazione alla competenza primaria o prevalente sull'intervento da porre in essere, mentre nel caso in cui l'accordo interessi due o più Regioni confinanti la promozione competerà alla Presidenza del Consiglio dei Ministri.
Le amministrazioni che invece vi dovranno partecipare sono individuate dalla norma in quelle che hanno un interesse all'oggetto dell'accordo; pertanto saranno legittimate innanzitutto le amministrazioni che risultino avere una competenza diretta e attiva in ordine agli interventi di cui all'accordo, nonché le amministrazioni che vedono rientrare l'oggetto dell'accordo nell'ambito delle materie o dell'insieme di interessi pubblici di loro competenza; allo stesso modo sono da ritenersi legittimate le amministrazioni che svolgono funzioni di vigilanza o controllo estrinsecantesi in provvedimenti autorizzatori nel caso in cui esse svolgano valutazioni propriamente discrezionali anche da un punto di vista tecnico.
La norma in esame individua quattro fasi procedimentali per addivenire alla costituzione di un accordo di programma.
La prima fase, quella dell'iniziativa, consiste nella promozione della conclusione dell'intesa, attraverso la convocazione di una conferenza di servizi fra tutti i rappresentanti delle amministrazioni interessate.
Nella seconda fase, quella istruttoria, la conferenza dei servizi esamina la possibilità e l'opportunità di stipulare un accordo e ne individua i contenuti.
La terza fase consiste nella stipula dell'accordo.
Infine, il procedimento si conclude con l'approvazione da parte del soggetto che si è fatto promotore delle trattative.

La norma prevede che nell'accordo le amministrazioni interessate debbano individuare tempi, modalità, finanziamenti e ogni altro connesso adempimento per perseguire l'obiettivo prefissato, fermo restando che le misure individuate dovranno essere coerenti con i fini di coordinamento ed integrazione tra le amministrazioni e che comunque non sarà possibile attraverso di esso eludere il principio di legalità dell'azione amministrativa.
La vigilanza sull'esecuzione dell'accordo di programma e gli eventuali interventi sostitutivi sono svolti da un collegio presieduto dal presidente della Regione o dal presidente della provincia o dal sindaco e composto da rappresentanti degli Enti locali interessati, nonché dal commissario del Governo nella Regione o dal prefetto nella provincia interessata se all'accordo partecipano amministrazioni statali o enti pubblici nazionali.
La norma in esame infine, prevede la possibilità di deferire ad apposite procedure arbitrali le eventuali controversie insorte tra gli enti partecipanti.

4.4 CRITERI PER LA REDAZIONE DEL PROTOCOLLO D'INTESA, DEL CONTRATTO E DEL CAPITOLATO TECNICO

Nel presente paragrafo è illustrata una soluzione per l'acquisizione di servizi di continuità operativa che si basa sull'ipotesi che vede più amministrazioni operare congiuntamente al fine di condividere l'acquisizione e la fruizione di servizi di continuità operativa. Conseguentemente, in relazione a tale ipotesi gli esempi di atto forniti – e che sono, come detto, allegati in appendice alle presenti Linee guida – consistono in un modello di:

- protocollo d'intesa, sottoscritto da tutte le amministrazioni interessate, che disegna il percorso da seguire al fine dell'espletamento in via congiunta della procedura di selezione del contraente, nonché alcuni modelli organizzativi finalizzati alla migliore gestione dell'iniziativa comune;
- contratto per l'acquisizione di servizi di continuità operativa;
- capitolato tecnico.

Si sottolinea che:

- tale soluzione è di applicazione generale, cioè non "dedicata" ad una particolare tipologia di amministrazioni;
- i modelli (ad eccezione, ovviamente, del protocollo) sono facilmente adattabili al caso in cui un'amministrazione intenda procedere singolarmente.

Con riferimento all'acquisizione congiunta di servizi operativi da parte di più amministrazioni ed alla relativa struttura tecnicamente condivisa, va peraltro fatto presente che, mentre nel capitolato è possibile fare riferimento a tale insieme sotto il profilo, appunto, tecnico, nel contratto andrà comunque ricordato che il rapporto giuridico viene posto in essere con il fornitore sempre e comunque dalla singola amministrazione facente parte del richiamato insieme.
Deve essere inoltre chiaro che tutti gli esempi di modelli sono esclusivamente indicativi e non vanno intesi come testi precompilati da utilizzare così come presentati.

Si sottolinea inoltre che il protocollo, il contratto ed il capitolato tecnico fanno riferimento a tutte le classi di servizio rappresentative della totalità dei servizi che costituiscono la continuità operativa e cioè:

- servizi di progettazione/realizzazione della soluzione di continuità operativa;
- servizi di manutenzione delle componenti hardware;
- servizi di conduzione sistemistica e operativa post-realizzazione della soluzione di continuità operativa;
- messa a disposizione di spazi informatici attrezzati e gestiti;
- servizi di risorse elaborative.

Nello Studio di fattibilità/Capitolato tecnico le amministrazioni, in base alle rispettive singole esigenze, configureranno la soluzione ritenuta più congrua, richiedendo l'acquisizione di tutte o parte delle citate classi di servizio.

4.4.1 Il Protocollo d'intesa

La finalità di tale atto è quella di formalizzare l'impegno delle amministrazioni a procedere alla effettuazione dello Studio di fattibilità ed alla successiva realizzazione di un Centro condiviso di continuità operativa dedicato alle amministrazioni sottoscriventi il protocollo medesimo.
A tal fine si prevede la costituzione di:

- un Comitato di Coordinamento (CdC) che svolge le funzioni di indirizzo, governo, monitoraggio e controllo dello sviluppo ed avvio del progetto;
- un Comitato Tecnico (CT) che svolge la funzione di indirizzo tecnico nella realizzazione del Progetto; in particolare il CT predispone le proposte tecniche per la realizzazione del Progetto e supporta il CdC.

4.4.2 Il Contratto

Il Contratto definisce le modalità, condizioni e termini generali in base ai quali il Fornitore assume l'obbligo di fornire alla singola amministrazione, parte del contratto, l'insieme degli specifici servizi necessari per garantire alla stessa la continuità operativa, tenendo altresì conto degli elementi di condivisione della soluzione medesima.

4.4.3 Il Capitolato

Il Capitolato non prevede particolari clausole ma tiene conto, ovviamente, delle classi di servizio e delle tipologie di livelli di servizio connessi previsto nel modello di contratto.

4.5 L'accordo di mutuo soccorso

Di seguito, al fine di fornire una guida alla stipula di un accordo di mutuo soccorso, vengono elencati ed illustrati brevemente alcuni elementi tipici di tale tipo di accordo relativo ai servizi informatici.
Si precisa che le clausole dell'accordo dipendono essenzialmente da ciò che viene concordato dalle parti in merito alla tipologia ed i livelli di mutua assistenza. Pertanto le indi-

cazioni che seguono devono essere considerate semplicemente come gli elementi di partenza per discutere, condividere e formalizzare l'accordo vero e proprio.

4.5.1 CLAUSOLE GENERALI

Ambito di applicazione
Definisce il contesto cui l'accordo si riferisce, identificando le organizzazioni, le sedi e le tipologie di attività o servizi. Nel caso l'accordo per la continuità operativa faccia parte di un più ampio accordo di mutua assistenza relativo ad altri settori (energia, tutela del patrimonio artistico, ecc.), è opportuno farne esplicita menzione.
Ad esempio:

> *l'accordo si inserisce nel piano di reciproca assistenza di cui al protocollo d'intesa … del … e riguarda la collaborazione per la continuità dei servizi informatici degli enti firmatari di seguito riportati, con riferimento alle sedi operative site sul territorio nazionale.*

Oggetto dell'accordo
Stabilisce i termini dell'accordo. È opportuno precisare la tipologia di accordo sia per quanto riguarda il tipo di assistenza che ciascuna parte si impegna a fornire, sia relativamente ai servizi cui l'assistenza si riferisce.
Ad esempio:

> *ciascuna parte si impegna a fornire la migliore assistenza possibile nel caso l'altra parte si trovi in una circostanza calamitosa che comporti l'interruzione dei servizi informatici essenziali per un periodo di tempo significativo. L'assistenza sarà finalizzata a consentire il ripristino dei servizi informatici essenziali mediante risorse strumentali alternative che saranno approntate all'occorrenza secondo il piano di continuità operativa. La parte soccorritrice renderà disponibili i locali, gli apparati informatici ed i collegamenti telematici, nei limiti delle proprie disponibilità, fatte salve le esigenze di continuità dei propri servizi informatici.*

Impegno economico
Va precisato l'eventuale impegno economico che l'accordo prevede per ciascuna parte.
Di norma questi accordi sono a titolo non oneroso, in tal caso è opportuno inserire una clausola del tipo:

> *le parti convengono che i vantaggi derivanti dalla mutua protezione rappresentano adeguata ricompensa per le eventuali attività straordinarie svolte ai fini del soccorso, pertanto non è dovuto compenso alcuno per i servizi resi nell'ambito del presente accordo.*

Se i firmatari dell'accordo decidono invece di prevedere un compenso forfetario per le attività di soccorso, è necessario specificarlo in questa clausola:

> *a titolo di parziale ristoro degli oneri sostenuti dall'organizzazione soccorritrice per l'espletamento delle attività di propria competenza previste nel presente accordo e nel piano di continuità operativa, l'organizzazione in emergenza che venga ospitata dal-*

l'organizzazione soccorritrice verserà a quest'ultima un contributo forfetario ed omnicomprensivo di euro ...... (......) con le modalità di seguito riportate ...

Periodo di validità dell'accordo
È opportuno venga sempre indicato un periodo di validità dell'accordo (3-7 anni). Scaduto il termine, le parti potranno rinnovare l'accordo modificandone eventualmente le condizioni.

Recesso
Va indicata la possibilità di recesso dall'accordo. Di regola ciascuna parte può recedere dall'accordo in qualunque momento, senza necessità di motivare tale decisione, dandone comunicazione scritta alle altre parti.
Può essere previsto un periodo di preavviso prima del recesso.

Responsabilità delle parti in caso di recesso
Questa clausola riporta le responsabilità delle parti in caso di recesso dall'accordo oppure per il mancato o parziale intervento a seguito di una formale richiesta di soccorso.
Di norma i patti di mutuo soccorso non prevedono alcuna responsabilità[49]:

nessuna delle parti firmatarie è responsabile nei confronti delle altre parti per gli effetti derivanti dal recesso dal presente accordo; le parti non sono altresì responsabili per le conseguenze dovute a carenza o difformità di assistenza rispetto a quanto previsto nel presente accordo.

4.5.2 CLAUSOLE CHE REGOLAMENTANO LE ATTIVITÀ DI MUTUO SOCCORSO

Prove periodiche
Nel caso si prevedano prove periodiche congiunte, è opportuno venga sempre indicato un periodo di validità dell'accordo (3-7 anni):

le parti concordano di eseguire prove congiunte dei rispettivi piani di continuità operativa al fine di verificarne l'efficacia. Le prove si svolgeranno almeno con cadenza annuale simulando a turno la condizione di crisi per ciascuna organizzazione aderente al presente accordo.

Modalità di richiesta del soccorso
Deve essere esplicitato il modo in cui sarà richiesta l'attivazione del processo di soccorso. In particolare è opportuno stabilire:

- i soggetti autorizzati ad inoltrare la richiesta di soccorso (vertice dell'organizzazione, responsabile della sicurezza, soggetto terzo, ecc.);
- la procedura con cui sarà inoltrata la richiesta (ad esempio tramite chiamata telefonica confermata entro 24 ore da una richiesta scritta);

[49] Si vuole osservare che, benché l'assenza di responsabilità possa fare apparire l'accordo particolarmente "debole", all'atto pratico la naturale solidarietà che si manifesta in occasione di eventi calamitosi rende il patto efficace. Ciò nondimeno è possibile prevedere alcune responsabilità per rendere l'accordo maggiormente vincolante.

- le informazioni che devono accompagnare la richiesta di soccorso (motivazione della richiesta, tipologia di servizi necessari, punti di contatto, ecc.).

Organizzazione soccorritrice
Nel caso l'accordo riguardi più di due organizzazioni, è opportuno chiarire la logica con cui sarà individuata l'organizzazione soccorritrice. Le possibilità sono:

- scelta autonoma dell'organizzazione in emergenza;
- scelta secondo una logica predeterminata (ad esempio secondo una scala di priorità basata sulle distanze geografiche tra i siti);
- scelta effettuata da un ente terzo che svolge il ruolo di coordinatore dei soccorsi.

È anche opportuno concordare se la stessa richiesta di soccorso possa essere inoltrata contemporaneamente a più enti.

Compiti del destinatario di una richiesta di soccorso
Vanno descritti gli impegni assunti dall'organizzazione che riceve una richiesta di soccorso. Ad esempio:

l'organizzazione che riceve richiesta di assistenza intraprenderà, secondo il piano temporale concordato con la parte richiedente, le azioni necessarie per ripristinare i servizi informatici essenziali ed a tal fine renderà disponibili i locali, gli arredi, gli apparati, i materiali e le altre risorse occorrenti per erogare il servizio in condizioni di emergenza[50].

Condizioni di deroga agli obblighi di soccorso
Vanno elencate le eventuali condizioni che sollevano l'organizzazione che riceve una richiesta di soccorso dagli obblighi di cui al punto precedente.
Ad esempio:

- *l'organizzazione che riceve richiesta di assistenza non è tenuta a svolgere le attività richieste se:*
  - *è anch'essa in uno stato di emergenza, per un evento calamitoso o altre cause impreviste;*
  - *ha già avviato una procedura di soccorso a favore di altro ente che partecipa all'accordo.*

Comitato di crisi
Può essere opportuno prevedere la costituzione di un comitato di crisi che comprenderà sia esperti dell'organizzazione in stato di emergenza che dell'organizzazione soccorritrice. Il comitato di crisi può essere costituito anticipatamente (soluzione consigliabile) o al momento in cui si verifica la condizione di emergenza. Tra i compiti tipici del comitato di crisi:

- la validazione dei piani di continuità operativa;

[50] L'elenco delle risorse che saranno rese disponibili in condizioni di emergenza può essere contenuto in un documento, concordato tra le parti, redatto in occasione della definizione del piano d'emergenza ed aggiornato periodicamente: in questo caso la clausola relativa agli obblighi può fare esplicito riferimento a tale documento.

- la pianificazione ed il controllo delle eventuali prove;
- il coordinamento delle attività relative al recupero dei dati, il ripristino dei servizi, l'esercizio in condizioni di emergenza ed il rientro alla normalità.

Coordinamento delle attività

È opportuno precisare la responsabilità del coordinamento delle attività che saranno svolte durante le prove ed in condizioni di emergenza. L'approccio tipico consiste nel definire una struttura di coordinamento cui partecipano sia l'ente in emergenza che quello ospitante. Tale struttura può coincidere con il comitato di crisi.
Ad esempio:

> *le attività relative al ripristino dei servizi informatici, la loro erogazione in condizioni di emergenza ed il rientro alle condizioni ordinarie, saranno coordinate dal comitato di crisi di cui al punto … Il personale della parte soccorritrice incaricato delle attività di assistenza, pur conservando l'organizzazione ed i riporti correnti, opererà coerentemente con le indicazioni fornite dal comitato di crisi.*

Durata massima dell'attività di soccorso

Si tratta di una clausola molto importante perché salvaguarda l'amministrazione soccorritrice da una permanenza eccessiva dell'ente in emergenza presso il proprio sito.
In genere viene indicato un termine massimo, trascorso il quale l'organizzazione in emergenza è tenuta ad abbandonare il sito ospitante.
Una soluzione alternativa consiste nel prevedere che le due organizzazioni (o il comitato di crisi) sviluppino concordemente un piano di rientro che terrà conto delle specificità del disastro: in tale caso l'organizzazione in emergenza si impegna a rispettare i tempi di tale piano.

4.5.3 CLAUSOLE DI TUTELA

Riservatezza delle informazioni

È opportuno che le parti si impegnino a non divulgare le informazioni di cui verranno a conoscenza nell'espletamento delle attività di mutuo soccorso:

> *le parti sono tenute ad assicurare la riservatezza delle informazioni, dei documenti e degli atti amministrativi dei quali vengano a conoscenza durante l'esecuzione del presente accordo ed inoltre si impegnano a rispettare rigorosamente tutte le norme relative alla tutela della riservatezza dei dati personali.*

Limiti di applicabilità dell'accordo

Può essere utile introdurre una clausola che tuteli nei confronti di un uso "improprio" dell'accordo, ad esempio per utilizzare senza compensi la consulenza di esperti di un'altra organizzazione.
Ad esempio:

> *il presente accordo non può essere utilizzato in alcun modo per giustificare attività o accordi tra le organizzazioni, o tra il personale delle medesime, che siano al di fuori del mero obiettivo di reciproco soccorso a seguito di eventi imprevisti e calamitosi.*

Responsabilità nei confronti di terzi
Occorrerebbe definire le responsabilità delle parti relativamente ad eventuali danni che possono essere arrecati a terzi nel periodo in cui l'organizzazione soccorritrice ospita l'organizzazione in emergenza.
In generale è tutelata l'organizzazione ospitante che non è responsabile per i danni arrecati in conseguenza dei servizi erogati in condizioni di emergenza, a meno che essi non siano dovuti a comportamenti negligenti o malevoli del proprio personale.

Interpretazione dell'accordo
Può essere utile prevedere una modalità operativa per risolvere controversie derivanti da una diversa interpretazione dell'accordo.
Ad esempio:

> *qualora dovessero insorgere difformità interpretative tra le parti in ordine alle disposizioni e clausole contenute nel presente accordo, le parti medesime concordano che provvederanno alla bonaria risoluzione delle difformità di cui sopra mediante appositi incontri che saranno fissati allo scopo di raggiungere un'interpretazione comune; qualora non dovesse essere raggiunta una posizione comune tra le parti, le medesime rimetteranno la decisione ad un Collegio arbitrale composto da tre membri di cui due nominati dalle parti in contenzioso, ed il terzo di comune accordo dagli arbitri nominati dalle parti.*

5. Le tecnologie per la continuità operativa

Si può asserire che non esistono tecnologie specifiche per la continuità operativa poiché, individuato l'obiettivo di recupero, qualunque tecnologia è utilizzabile.
Più che parlare di tecnologie per la continuità operativa, bisognerebbe parlare di tecnologie in genere, in quanto ciascuna tecnica (informatica o tradizionale) può essere utilizzata per realizzare processi di recupero dell'operatività eventualmente presso centri alternativi.
Ad esempio in un sito di backup possono essere utilizzate, ai fini della continuità operativa, tutte le tecnologie informatiche presenti nel sito primario, spaziando da quelle più tradizionali (elaborazione, gestione dati, servizi di comunicazione) alle più innovative (*web services, mobile computing*, ecc.).
Ciò nondimeno alcune scelte tecnologiche facilitano più di altre la realizzazione di una soluzione di continuità operativa, in quanto semplificano le attività necessarie per ripristinare i servizi a seguito di un evento imprevisto.
In particolare, si può distinguere tra:

- tecnologie che semplificano il salvataggio dei dati e limitano la perdita di informazioni in caso di disastro (backup e replica dei dati);
- soluzioni che migliorano la capacità di un sistema informatico di mantenere l'operatività anche a seguito di problemi circoscritti e di eventi calamitosi (affidabilità della rete, virtualizzazione dei dati);
- tecniche che mirano a ridurre il tempo di ripartenza in caso di evento disastroso (*hot standby*, cluster remoto dei sistemi).

Nel seguito viene presentata un panoramica di tali tecnologie evidenziando come esse possano essere impiegate per rendere più efficaci le soluzioni di continuità operativa.

5.1 Il backup dei dati

Le procedure di salvataggio e conservazione dei dati, comunemente dette procedure di backup, sono indispensabili per realizzare qualunque soluzione di continuità operativa.
I nastri sono i supporti tradizionalmente utilizzati per le attività di backup, in ragione della loro elevata capacità di immagazzinamento dati e semplicità di trasporto.
Nonostante il costante progresso dei supporti di memorizzazione magnetici ed ottici, i nastri restano ancora oggi il mezzo preferito per il salvataggio dei dati e la loro conservazione ai fini di un eventuale ripristino.

5.1.1 I NASTRI MAGNETICI LTO

Il nastro magnetico è oggi la soluzione che permette di fare copie dati al più basso dei costi possibili e che, per la sua natura di tecnologia sequenziale, indirizza le esigenze di continuità operativa dove i tempi di ripristino richiesti dal servizio (RTO) sono di ore o giorni.
Nel 1998 un consorzio di tre società (IBM, HP e Seagate) decise di proporre un formato standard al fine di superare il problema di incompatibilità delle tecnologie allora presenti sul mercato. Il risultato di tale collaborazione è stato lo sviluppo della tecnologia LTO (*Linear Tape Open*) che si è poi di fatto affermata sul mercato come la migliore per gli ambienti eterogenei.
I principali vantaggi di tale tecnologia sono:

- standard pre-definito della cartuccia nastro che permette l'interscambio della cartuccia stessa tra unità nastro di vari fornitori che aderiscono allo standard;
- certificazione, da parte di un ente indipendente, della conformità allo standard delle cartucce e delle unità nastro, attestata dall'utilizzo del logo "Ultrium-LTO";
- strategia di sviluppo dello standard che garantisce agli utenti continui miglioramenti in termini di capacità e velocità di trasferimento dati, al fine di far fronte ad esigenze sempre in crescita (cfr. Tabella 15);
- regole della compatibilità all'indietro, al fine di poter leggere/scrivere cartucce con tecnologia n-1.
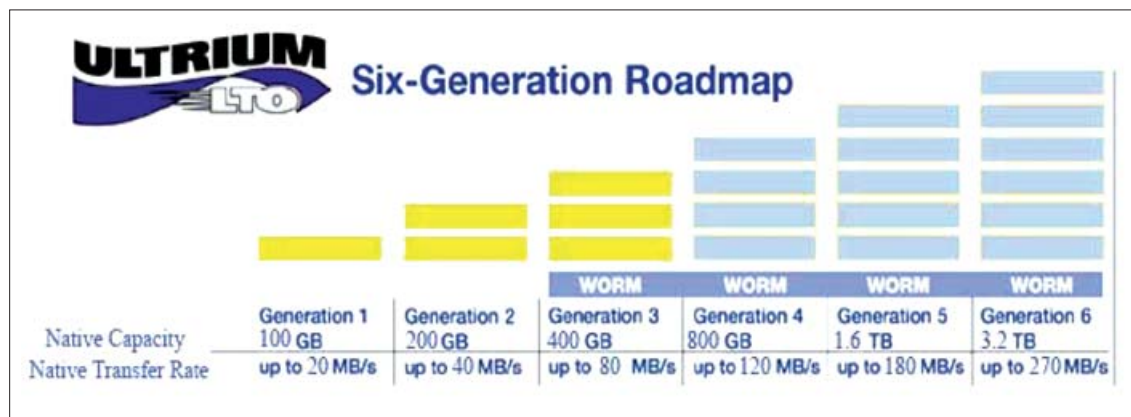
Tabella 15 - Piano di evoluzione della tecnologia LTO

In Tabella 15 è evidenziato il percorso di evoluzione dei nastri che aderiscono allo standard LTO: le colonne contrassegnate in giallo riportano le caratteristiche raggiunte finora mentre le colonne in azzurro riportano i progressi previsti per le generazioni future.
Un importante obiettivo di progetto è inoltre fornire una soluzione di qualità idonea al backup e sopratutto al restore in caso di necessità dei dati salvati. A questo scopo LTO è dotato di una serie di caratteristiche di progetto per l'alta affidabilità e la protezione dei dati memorizzati:

- *Leader-Pin:* il dispositivo di aggancio del nastro magnetico é in metallo con possibilità di rottura praticamente nulle (rispetto, per esempio, alla cartuccia DLT con *leader-pin* di plastica);

- Servo-tracce: consente alla testina di posizionarsi con estrema precisione sul nastro ed è una particolarità assolutamente unica per i prodotti di questa fascia di mercato, che assicura maggiore precisione di lettura e di scrittura. Le servo-tracce vengono scritte sul nastro in fase di produzione e inviano alla testina di lettura/scrittura dei segnali elettronici che ne garantiscono il perfetto posizionamento;
- dispositivo ECC (*Error Correction Control*): permette di recuperare dati danneggiati o perduti, consentendone la ricostruzione sulla base delle informazioni ancora disponibili.

La tecnologia LTO è oggi disponibile con un'offerta molto modulare e utilizza sempre lo stesso media magnetico. Ogni fornitore interpreta lo standard con soluzioni di funzionalità più o meno sofisticate e quindi con costi differenziati. Le librerie disponibili sul mercato differiscono per numero di *slots* (cartucce) disponibili e *drive* (testine di lettura) che possono operare in parallelo.
Le unità LTO possono collegarsi a un numero estremamente vasto di ambienti operativi, assicurando una crescita senza necessità di cambiare tecnologia, inconveniente che spesso è accaduto o accade ancora con altre tecnologie.
Oggi è disponibile la tecnologia LTO di generazione 3 con cartucce da 400GB e velocità di trasferimento fino a 80MB/sec. LTO3 introduce inoltre la funzionalità WORM (*Write Once Read Many*) che garantisce la non modificabilità dei dati scritti su cartuccia. Tale funzionalità è particolarmente interessante per l'implementazione di nuove soluzioni legate all'archiviazione di dati sensibili e/o di natura legale/fiscale, come ad esempio le cartelle cliniche dei pazienti, le fatture, o le e-mail di natura commerciale, sempre più utilizzate per effettuare compravendita di beni, azioni o definire rapporti contrattuali.
Si segnala che la generazione 4 di LTO prevede l'uso della crittografia sui nastri come ulteriore elemento di sicurezza quando i nastri vengono trasportati all'esterno.
Il consorzio LTO mantiene un sito aggiornato con le ultime novità e documentazioni di supporto:

- http://www.ultrium.com/newsite/index.html

5.1.2 I NASTRI VIRTUALI

Una evoluzione del backup su nastro tradizionale consiste nell'utilizzo di nastri virtuali (*virtual tape*).
Questa soluzione combina le metodologie tradizionali di salvataggio su nastro con la tecnologia di scrittura su disco magnetico, al fine di realizzare una soluzione di backup e di recovery ottimizzata. Si tratta di un sistema che emula i dispositivi a nastro tradizionali e consente di utilizzare le procedure di salvataggio su nastro beneficiando della elevata velocità dei supporti magnetici.
Una libreria di nastri virtuali si presenta alle applicazioni come una serie di librerie fisiche, ognuna con i propri lettori (drive) ed il proprio pool di nastri. Essa è composta dai seguenti componenti:

- 1 o più *engine* ovvero server con il motore di virtualizzazione;
- 1 o più *cache controller module*, con controller RAID e dischi (SATA);
- il software con le licenze necessarie a gestire tutta la cache disco configurata e le funzioni a valore aggiunto.

Questa tecnica è indicata per le soluzioni di continuità operativa in cui si vuole coniugare la semplicità e versatilità delle procedure su nastro con l'efficienza e l'affidabilità dei dispositivi di memorizzazione magnetici.
Tra le possibilità offerte dalla registrazione su disco ricordiamo:

- la possibilità di impiego di prodotti che automatizzano le funzioni di backup e di recovery;
- la possibilità di impiego di dispositivi di elevata affidabilità (dischi RAID);
- la possibilità di duplicare ed eventualmente "remotizzare" i dischi aumentando la resilienza ai problemi di continuità operativa.

Spesso i nastri virtuali sono utilizzati come un sistema di salvataggio "di transito" a sua volta impiegato per salvare i dati fuori linea sui supporti a nastro tradizionali.

5.1.3 IL BACKUP REMOTO

Per assicurare la continuità operativa i dati di backup devono essere conservati in modo da garantire la loro disponibilità anche a seguito di eventi che rendono inagibile il sito primario. La soluzione che di solito si adotta è quella di conservare le informazioni di backup in un sito remoto.
È possibile adottare due diversi metodi:

- il trasporto delle copie dei supporti contenenti il backup presso il sito remoto;
- la scrittura diretta delle informazioni di backup presso un sistema di memorizzazione presente nel sito remoto.

Quest'ultimo metodo prende il nome di backup remoto e consiste nell'impiego di tecniche che consentono di scrivere su archivi remoti sfruttando le capacità trasmissive della rete.
La soluzione utilizza server dedicati al backup opportunamente connessi in rete (ad esempio è possibile utilizzare server del tipo NAS – *Network Attached Storage*).
Tali server possono essere parte del sistema informatico oppure possono esser gestiti da società che offrono servizi di backup remoto: in quest'ultimo caso la società che offre servizi assicura anche la corretta conservazione dei dati, sollevando il cliente dalle attività di gestione dei supporti e delle informazioni di backup.
Spesso si utilizzano tecniche che producono una doppia copia di backup: una locale, l'altra remota[51]. In questo caso occorre integrare alle funzioni di backup remoto con opportune tecniche che garantiscono l'allineamento delle copie, comunemente note come tecniche di replica dei dati.

5.1.4 LA REPLICA DEI DATI

Le tecniche di replica dei dati sono da tempo utilizzate per incrementare la distribuzione e la disponibilità dei dati sia ai fini prestazionali, sia per motivi di sicurezza. I prodotti che offrono funzioni di replica sono molteplici e comprendono i DBMS, i sistemi di gestione dello storage e prodotti di sicurezza specifici.

[51] Le copie di backup sono utilizzate non solo per la continuità operativa, ma anche per problemi di sicurezza e di qualità: in questi casi le procedure di recupero sono più efficienti partendo da una copia locale.

Dal punto di vista delle tecnologie, le tecniche di replica possono essere trattate in relazione al metodo con cui la replica viene prodotta ed al tipo di dato che viene replicato.
Per quanto concerne il primo aspetto, le repliche possono distinguersi in fuori linea ed in linea, queste ultime si dividono a loro volta in asincrone e sincrone.
Le repliche fuori linea vengono prodotte ad intervalli predeterminati (ad esempio ogni ora) o in occasione di eventi particolari (ad esempio dopo il passaggio di una determinata procedura). Le repliche ottenute con tale modalità sono sempre in uno stato congruente, ma vengono aggiornate in modo discontinuo per cui possono corrispondere ad uno stato non aggiornato della base dati.
Nelle repliche in linea l'aggiornamento è invece continuo, avviene cioè man mano che i dati primari vengono modificati. Se la replica è di tipo asincrono, l'aggiornamento delle copie primarie e secondarie procede in modo indipendente e con una lievissima sfasatura temporale, invece nel caso di replica sincrona i due aggiornamenti vengono coordinati per fare in modo che in qualunque momento le copie primarie e secondarie siano allineate e congruenti[52].
Relativamente alla tipologia di dato replicato il mercato offre soluzioni che vanno dalla semplice replica dalle strutture dati presenti nei dispositivi di memorizzazione (replica di tipo fisico) a tecniche di duplicazione dei dati secondo vari formati e diversi livelli di astrazione (volume, file, tabella, data base, metadati, ecc.).
Combinando questi aspetti tecnologici, eventualmente in modo diverso in relazione alla tipologia di informazione, si possono avere svariate soluzioni per la continuità operativa.
I principali fornitori di prodotti hardware e software e gli integratori di sistema propongono oggi sistemi di replica che utilizzano le tecniche elencate in specifiche soluzioni commerciali, spesso di carattere proprietario, talvolta integrate nei sistemi di virtualizzazione dei dati.

5.1.5 La copia locale e la replica fuori linea

Le copie locali dei dati (disponibili nei prodotti commerciali con varie denominazioni: *point in time copy, flashcopy, snapshot, volume copy, instant copy*, etc.) tipicamente vengono utilizzate per realizzare una fotografia dei dati in un particolare istante del processo di elaborazione come, ad esempio, la chiusura della sessione di lavoro giornaliera, il completamento di una applicazione *batch*, ecc.
Si tratta di copie di backup che sono utilizzate principalmente per proteggere i dati e ripristinare i servizi in caso di problemi ordinari o di eventi eccezionali che non comportano la distruzione del sistema informatico.
Alcuni prodotti sono in grado di produrre una copia dei dati senza fermare le operazioni di scrittura. A tal proposito occorre tenere presente che molto spesso i dati relativi ad un volume[53] utilizzato da un'applicazione non sono necessariamente tutti sul sistema storage al momento in cui viene richiesta la copia ma potrebbero essere anche nella memoria dell'elaboratore (p.es. *buffer pool*). Questo implica che una copia istantanea consistente può essere fatta solo quando l'applicazione ha terminato l'utilizzo del volume oppure quando

[52] La terminologia utilizzata in letteratura non è sempre omogenea; ad esempio alcuni definiscono come "asincrone" le repliche fuori linea e come "quasi-sincrone" le repliche in linea di tipo asincrono.

[53] In questo contesto il termine "volume" indica l'unità Input/Output referenziata dall'applicazione.

il software di sistema ed il DBMS sono integrati con il software che gestisce il processo di copia (in sostanza il DBMS viene avvisato della richiesta di copia istantanea, scarica i dati su disco e autorizza la copia istantanea). Il principale beneficio della scelta di prodotti integrati è la possibilità di effettuare copie di backup durante le attività correnti, minimizzando l'impatto sul servizio offerto.
Ai fini della continuità operativa, per rendere possibile il recupero anche nel caso di distruzione delle copie locali, di norma viene realizzata una replica fuori linea, consistente in una copia ulteriore "istantanea"[54] su nastro che viene poi in differita trasportata verso l'esterno.
Questo processo ha il vantaggio di combinare le tecniche di backup con quelle della replica dei dati. Vengono infatti utilizzati i processi tipici del backup, caratterizzati da elevata affidabilità e tempi ridotti di fermo delle applicazioni, ma al tempo stesso è possibile produrre le copie di sicurezza eseguendo in tutta comodità la replica su nastro in differita.
Molti prodotti che eseguono copie dei dati di tipo logico (ad esempio, i DBMS) effettuano anche la registrazione continua degli aggiornamenti su opportuni file sequenziali chiamati log.
In caso di necessità, disponendo dei log degli aggiornamenti, sarà possibile ripristinare la base informativa all'ultimo salvataggio effettuato e portarla ad uno stato aggiornato riapplicando gli aggiornamenti registrati nei log. Nel caso invece un evento calamitoso distrugga le copie primarie ed i log degli aggiornamenti, sarà possibile utilizzare le copie di sicurezza per portare il sistema secondario ad uno stato che potrebbe essere rimasto indietro in termini di aggiornamenti (RPO>0).

5.1.6 La replica in linea dei dati

Le tecniche di replica in linea dei dati consentono di rendere praticamente nulla la perdita di informazioni, anche in caso di eventi che distruggano le copie primarie ed i log (RPO=0).
Nella replica "sincrona", l'applicazione che richiede l'operazione di scrittura di un dato riceve la conferma dal sistema dopo che il dato è stato scritto con successo nel sistema storage primario (presso il sito locale) e nel sistema storage secondario (presso il sito remoto).
Tale scrittura avviene di solito nelle memorie cache dei due sistemi storage. Per questo motivo i sistemi di memorizzazione sono di solito ridondati e dotati di batterie tampone, al fine di garantire in ogni caso la scrittura su disco fisico. Questa tecnica ha il vantaggio di garantire il sincronismo degli aggiornamenti, ma costringe le applicazioni ad "aspettare" la doppia scrittura, dunque condiziona le prestazioni e la disponibilità dei servizi al carico di entrambi sistemi storage interessati, al tempo di propagazione del dato in rete, alla ampiezza di banda del collegamento verso il sito remoto ed alla disponibilità della rete.
Per questi motivi le repliche di tipo sincrono sono efficienti solo in ambiti con reti di elevata qualità, pertanto vengono utilizzate in configurazioni "campus"[55] e per distanze nell'ordine delle decine di chilometri.

---

[54] In letteratura queste copie sono spesso referenziate con l'espressione inglese *Point In Time*.

[55] Le configurazioni di questo tipo sono quelle in cui non si è vincolato all'utilizzo di servizi di comunicazione esterni ed è pertanto possibile realizzare reti specifiche con elevate caratteristiche qualitative.

Per distanze maggiori si utilizzano di solito tecniche di replica dati remota di tipo "asincrono" dove l'applicazione scrive sul sistema primario e non aspetta la scrittura sul sito secondario che avviene in differita. Esistono esempi di replica dati remota in produzione tra siti distanti anche migliaia di chilometri. Ovviamente maggiore è la distanza maggiore è la garanzia di protezione da eventi disastrosi, ma maggiore sarà anche il costo dei collegamenti remoti. Occorre valutare, come sempre, costi e obiettivi di progetto.
Una considerazione fondamentale riguarda la consistenza dei dati tra sistemi primari e secondari. A titolo di esempio si consideri il caso di due sistemi primari condivisi dalla stessa applicazione replicati remotamente su due sistemi secondari: nel caso di copia asincrona gli aggiornamenti tra le quattro unità viaggiano in tempi diversi e quindi in caso di disastro nel sito primario alcuni dati potrebbero essere in transito mentre altri già arrivati. A questo problema si ovvia con una tecnologia chiamata "gruppi di consistenza" che è in grado di raggruppare aggiornamenti appartenenti alla stessa applicazione (anche su più sistemi primari) e trasferirli sui sistemi secondari, garantendo la corretta sequenza degli aggiornamenti e la completezza dei dati a quel momento. Questo consente una più veloce ripartenza dei sistemi secondari (riduzione RTO) e la garanzia che tutti i dati trasferiti con l'ultimo gruppo di consistenza siano completi (RPO predefinito).
Infine, esiste la possibilità di combinare le funzionalità sincrone e asincrone in una configurazione a tre siti dove due unità storage sono a distanza "campus" e dialogano in modalità sincrona e una terza unità storage si trova a distanza "geografica" e dialoga in modalità asincrona. Le prime due unità garantiscono il servizio in caso di fermo pianificato (p.es. manutenzione del sito primario) e da disastri ad impatto limitato (p.es. incendio o allagamento) la terza unità protegge da disastri di maggiore entità dal punto di vista della estensione territoriale (p.es. alluvioni, terremoti, etc.).

	VANTAGGI	SVANTAGGI
Replica in linea sincrona	• Copia primaria e secondaria sempre congruenti • È possibile realizzare soluzioni con tempi di ripartenza ridottissimi (RTO=0), idonee anche per problemi minori	• Costi di comunicazione elevati, soprattutto per grandi distanze • Impatta potenzialmente sulle prestazioni
Replica in linea asincrona	• Idonea anche per siti molto distanti (soluzioni efficaci anche nel caso di disastri di grande estensione) • Basso impatto sulle prestazioni	• Non è garantita la piena congruenza tra i dati presenti nel sito primario e secondario

Tabella 16

Rispetto alle tecniche di replica fuori linea, quelle in linea consentono di avere il sistema secondario aggiornato (RPO=0) anche nel caso in cui un evento calamitoso distrugga le copie primarie ed i log degli aggiornamenti[56], a prezzo di un elevato impegno delle linee di comunicazione.
Occorre comunque considerare che anche quando è possibile ripristinare la base informativa ad uno stato recente riapplicando gli aggiornamenti registrati nei LOG, è necessario un tempo consistente per il trasporto dei supporti contenenti i log presso il sito di recupero e per l'applicazione degli aggiornamenti alla base dati. Avere i dati perfettamen-

[56] Per la precisione la perdita nulla di dati (RPO=0) è garantita dalla sola replicazione sincrona, ma l'esperienza ha comunque dimostrato che, anche nel caso di replica asincrona, la quantità di dati che possono essere persi (RPO) è minima e può essere tollerabile nella maggior parte delle applicazioni di tipo commerciale.

te aggiornati presso il sito di recupero è invece una condizione necessaria affinché le applicazioni possano essere trasferite velocemente ai sistemi secondari assicurando sia il recupero di tutti i dati (RTO=0), sia la piena continuità operativa (RTO tendente a zero).

5.1.7 LA REPLICA LOGICA DEI DATI

La duplicazione dei dati può essere condotta a diverso livello di astrazione, replicando la struttura dati così come memorizzata nel dispositivo di memorizzazione o riproducendo le medesime informazioni del sito primario con differenti strutture dati.
Il primo tipo di replica offre la piena garanzia di compatibilità tra le applicazioni ed il sistema di memorizzazione, ma richiede che presso il sito secondario siano presenti gli stessi apparati di memorizzazione utilizzati nel sito primario.
Il secondo tipo di replica, comunemente nota come replica logica dei dati, è indipendente dai dispositivi di registrazione utilizzati e presenta alcuni vantaggi:

- permette di duplicare le sole informazioni necessarie per la continuità operativa, riducendo l'occupazione di spazio presso il sito secondario;
- può utilizzare tecniche di allineamento ottimizzate in termini di dati trasmessi;
- può replicare le informazioni nel formato più idoneo ai sistemi presenti presso il sito secondario.

La compatibilità delle repliche logiche con le applicazioni è elevata nel caso di sistemi omogenei e, grazie alla diffusione di protocolli standard per l'accesso alle informazioni, è garantita anche in molti ambienti eterogenei.
Per i vantaggi esposti, la replica di tipo logico è quella più utilizzata per le soluzioni di continuità operativa.
Si possono distinguere due famiglie di soluzioni per la replica logica dei dati:

- a livello transazionale;
- a livello di sistema di memorizzazione.

La prima classe di soluzioni si basa sull'utilizzo delle le funzioni di replica tipiche dei DBMS e realizza presso il sito secondario, una base dati congruente ed allineata con quella operativa presso il sito primario. Nei sistemi sincroni viene garantita la piena congruenza tra le due basi dati attraverso l'utilizzo del protocollo a due fasi (*two phase commit protocol*).
Questo tipo di replica ha il vantaggio di poter essere realizzata facilmente sfruttando le funzioni proprie dei DBMS commerciali, ma è efficace solo per le informazioni accedute tramite transazioni e non è idonea nei casi in cui occorre replicare informazioni che non sono gestite dal DBMS (ad esempio sistemi documentali o aree di lavoro per applicazioni individuali).
Le soluzioni che operano a livello di sistema di memorizzazione sono conosciute con il nome generico di *mirroring* dei dati e sfruttano le funzioni dei prodotti di virtualizzazione dei dati per replicare presso il sito secondario le informazioni di interesse per la continuità operativa.
Di seguito viene data una breve descrizione delle varie tecnologie e tecniche operative al momento disponibili per l'allineamento logico dei dati:

- *Vaulting:* consiste nel trasportare via rete i backup giornalieri ai dispositivi di recupero, riducendo così ore di trasporto se avviene un disastro. Tipicamente, i server

di produzione sono connessi via rete all'unità a nastro del sistema di recupero, sebbene talvolta siano richiesti host intermedi. Questa tecnologia prevede un servizio di *network on-demand* (alta banda per poco tempo) o una connessione di rete diretta, a seconda della quantità di dati da trasportare. Il *vaulting* riduce il RTO, ma non influenza il RPO.

- *Journaling:* consiste nel trasportare al sistema di recupero i cambiamenti al DB o al sistema di memorizzazione che sono avvenuti dall'ultimo backup (registrazioni di LOG), o in maniera continua o a intervalli predefiniti. Tipicamente viene realizzato mediante una rete dedicata e un server dedicato presso il sistema di recupero. Il *journaling* accorcia il RPO, e abbrevia anche il RTO, riducendo il tempo di trasporto richiesto per portare gli aggiornamenti al sistema di recupero.
- *Shadowing:* questa tecnica comporta il mantenimento di una replica del database o del file system, tipicamente catturando i cambiamenti in maniera continua e applicandoli al sistema di recupero. Lo *shadowing* è un processo asincrono, perciò richiede meno banda del *mirroring* sincrono. L'ampiezza di banda è uguale o più grande di quella richiesta dal *journaling*, ma la capacità hardware richiesta è maggiore. Il RTO viene ridotto in maniera significativa (generalmente tra una e le otto ore, a seconda del tempo necessario per applicare la lista dei cambiamenti), mentre il RPO diventa pari all'istante dell'ultimo aggiornamento ricevuto e applicato.
- *Mirroring:* consiste nel mantenere una replica del database o del sistema di memorizzazione, applicando i cambiamenti presso il sistema di recupero in maniera sincrona (anche con meccanismi di lock al sito primario). Come risultato, il RTO può essere ridotto (da 20 minuti ad alcune ore), mentre il RPO si riduce solo alla perdita delle transazioni non concluse (*non committed*). Poiché è sincrono, il *mirroring* richiede un'ampiezza di banda certamente maggiore dello *shadowing*. Un'ampiezza di banda insufficiente o un'alta latenza degradano la performance del sito di produzione. È richiesto un hardware dedicato al sistema di recupero (per esempio, sottosistemi server e/o dischi).

5.2 I collegamenti in rete

5.2.1 L'affidabilità della rete

Le soluzioni di continuità operativa sono strettamente legate alle caratteristiche di affidabilità e ridondanza degli apparati che realizzano la rete di trasporto sia a livello geografico che locale. L'efficienza ed efficacia dei metodi di connessione dei dispositivi di memorizzazione (DAS, SAN, NAS) dipende in maniera diretta dai meccanismi di recupero della rete che costituisce lo strato di trasporto.
Di seguito si vuole fornire una breve indicazione sulle tecnologie di trasporto più diffuse nell'ambito della continuità operativa, e dei relativi meccanismi di recovery in caso di caduta delle connessioni fisiche.

Lo sviluppo della tecnologia di trasporto su fibra ottica ha reso possibile l'estensione della separazione geografica tra i Data Center primario e secondario, con notevoli benefici di natura tecnica ed economica:

- *riduzione dei costi* per la trasmissione dei dati di storage a lunga distanza;
- *superamento dei limiti di banda* delle linee tradizionali (queste ultime supportano velocità di megabit per secondo mentre i protocolli di storage generano traffico dell'ordine dei gigabit per secondo);
- *superamento dei limiti di distanza* che caratterizzano i protocolli nativi di connessione dello storage (ad esempio nel caso di Fibre Channel, nato per la connettività tra data center locali, la massima distanza consentita è pari 100 Km).

Gli apparati con connessioni in fibra ottica permettono l'estensione dei sistemi di storage per distanze di centinaia ed anche migliaia di chilometri, consentendo la ridondanza dei percorsi di accesso ai dati.
Riportiamo nella tabella seguente le caratteristiche principali delle tecnologie di trasporto a livello ottico esistenti sul mercato:

Trasporto ottico	Protocollo di Storage	Caratteristiche tecniche
Wave Division Multiplexing (WDM)	Fibre Chanel ESCON Gigabit Ethernet	• Replicazione sincrona e asincrona dei dati fino a centinaia di chilometri • Supporta la replicazione ad alte performance senza perdita di dati
Synchronous Optical Network/Synchronous Data Hierarchy (SONET/SDH)	Fibre Channel Gigabit Ethernet	• Replicazione asincrona dei dati fino a migliaia di chilometri con RPO dell'ordine di minuti/ore • Replicazione sincrona dei dati a distanza fino a centinaia di chilometri senza perdita di dati

Tabella 17

Tra le tecnologie di multiplazione e trasmissione di più segnali portanti su fibra ottica a determinate lunghezze d'onda (WDM) citiamo il CWDM (*Coarse Wave Division Multiplexing*) che è disponibile sugli apparati *routing switch* delle reti locali. Il CWDM è limitato al protocollo Gigabit Ethernet e supporta fino a 8 lunghezze d'onda, ma è comunque caratterizzato da una notevole economicità rispetto ai corrispondenti apparati DWDM (*Dense Wave Division Multiplexing*). La tecnologia CWDM si affida sui meccanismi di recovery di livello 2 e 3 degli apparati di switching, nel caso di caduta ai link o di failure di uno degli apparati costituenti l'anello ottico.
Lo sviluppo e la diffusione della tecnologia Ethernet rende oggi possibili connessioni locali di tipo Fast, Giga e 10Gigabit in ambito LAN e WAN.

5.2.2 La continuità delle reti locali

Se si considerano le tecnologie per la continuità operativa in ambito reti locali, tutti i meccanismi di affidabilità e ridondanza degli apparati di switching e routing possono essere tenuti in conto per progettare configurazioni atte a recuperare l'operatività in caso di problemi agli apparati o alle linee.

Per quanto concerne la disponibilità degli apparati, si può fare affidamento sulle caratteristiche hardware degli apparati presenti sul mercato che oggi offrono:

- valori particolarmente elevati di MTBF (*Mean Time Between Failures*);
- disponibilità di CPU ridondata, alimentazione ridondata, moduli *hot-swappable*, aggregazione dei collegamenti (802.3ad ed estensioni proprietarie dei venditori).

Dal livello fisico si può passare ai meccanismi di livello 2 (*Data Link*), con i protocolli standard che assicurano il recupero della connettività in caso di caduta di collegamenti fisici o di rottura di apparati. I protocolli che offrono queste funzionalità sono:

- IEEE 802.1D (*Spanning Tree*);
- IEEE 802.1w (*Rapid Spanning Tree*).

In aggiunta ai protocolli standard, si possono prendere in considerazione i meccanismi proprietari che forniscono notevoli miglioramenti rispetto ai primi in termini di tempi di ripristino in caso di rottura, di utilizzo di tutta la banda disponibile sui collegamenti fisici e di semplicità configurativa e di gestione[57].

5.2.3 LA CONTINUITÀ DELLE RETI IP

Per quanto concerne il recupero delle connessioni a livello 3 (livello *network*) è possibile utilizzare le funzioni native dei protocolli di instradamento (*routing*) più comuni:

- routing statico;
- VRRP;
- RIP;
- OSPF con ECMP.

Le soluzioni proprietarie che alcuni produttori rendono disponibili permettono l'utilizzo di servizi di livello 2 in ambienti routed, garantendo il ripristino dei percorsi di rete con i tempi tipici del livello Data Link (gli algoritmi di livello 2 possono convergere con tempi inferiori al secondo, mentre un protocollo di livello 3 impiega diverse decine di secondi in maniera direttamente proporzionale alla complessità della topologia di rete).
Inoltre, per la continuità operativa sono da tenere in forte considerazione tutte le soluzioni che permettono la virtualizzazione degli indirizzi IP (ad esempio il VRRP), e consentono la realizzazione di architetture ridondate sia in modalità *active-active* sia *active-standby*.
A livello applicativo (livello 4-7 della pila ISO-OSI) esistono sul mercato apparati integrati (*appliance*) che consentono il bilanciamento del carico in modo trasparente rispetto ai servizi, con possibilità di sostituzione a caldo delle unità in panne senza interruzione del servizio. In questo ambito gli apparati di ultima generazione permettono di ottimizzare i servizi, proteggere dagli attacchi ed incrementare le prestazioni sia a livello LAN che WAN.
Gli algoritmi più sofisticati di bilanciamento a livello applicativo consentono di implementare funzionalità di bilanciamento a livello globale, ridirigendo le sessioni di lavoro verso sistemi geograficamente distribuiti e realizzando in maniera totale la virtualizzazione del servizio.

[57] Si ricorda comunque che l'utilizzo di protocolli proprietari comporta l'obbligo di avvalersi di apparati di uno stesso fornitore, se ne consiglia pertanto l'utilizzo solo in caso di effettiva necessità.

5.3 LA VIRTUALIZZAZIONE DEI DATI

Man mano che le architetture evolvono, si tende a separare le soluzioni tecniche per la gestione dei processi da quelle dedicate alla gestione della memoria su disco (storage). Di conseguenza i supporti di memorizzazione oggi non sono più semplici accessori degli elaboratori, ma costituiscono un vero e proprio sistema autonomo, spesso caratterizzato da un'architettura distribuita articolata e complessa.
L'adozione di scelte architetturali di questo tipo favorisce la realizzazione delle soluzioni di continuità operativa. Nella fattispecie i principali vantaggi sono:

- la possibilità di operare su storage ad elevata distanza;
- la disponibilità di funzioni native di backup remoto (*vaulting*);
- la semplicità di realizzazione di soluzioni di continuità operativa basate su registrazioni speculari (*mirroring*);
- l'elevata affidabilità e resilienza ai disastri locali;
- l'indipendenza dai supporti di memorizzazione che possono essere scelti in funzione delle specifiche strategie di salvataggio e ripristino.

In questo capitolo viene pertanto presentata una veloce rassegna delle tecniche di gestione dei dati in rete (*storage networking*).

5.3.1 METODI DI CONNESSIONE DEI DISPOSITIVI DI MEMORIZZAZIONE

Di seguito vengono elencati i più diffusi metodi per la connessione ai sistemi dei dispositivi di memorizzazione.

- *Dispositivi ad attacco diretto – Direct Attached Storage (DAS):* si tratta di dischi connessi direttamente al sistema elaborativo mediante un cavo.
- *Storage Area Network (SAN):* ricadono in questa tipologia i sistemi di memorizzazione accessibili attraverso una rete dedicata che collega in modo paritetico gli elaboratori con i diversi dispositivi di memorizzazione. Normalmente le SAN utilizzano connessioni in fibra ottica.
- *Network Attached Storage (NAS):* sono sistemi di memorizzazione accessibili mediante una rete non dedicata allo storage, di solito di tipo TCP/IP (locale o geografica). La modalità di accesso è orientata al reperimento o alla condivisione dei file ed utilizza protocolli idonei a questo tipo di applicazione (CIFS – *Common Interface File System* – comune in ambiente Windows e NFS – *Network File System* – utilizzato in ambiente Unix)[58]. Per questo tipo di sistema vengono anche utilizzati i termini *file server*, *filer*, o *NAS appliance*.
- *iSCSI*[59]: con questa modalità di connessione i dispositivi di memorizzazione sono connessi ad una rete TCP/IP ma, a differenza dei sistemi NAS, l'accesso ai dati avviene tramite comandi SCSI che leggono/scrivono blocchi di I/O.

[58] In questi sistemi l'applicazione accede ai file tramite i comuni protocolli applicativi e l'apparato NAS trasforma la richiesta in opportuni comandi verso i dispositivi di memorizzazione.

[59] La sigla iSCSI sta per Internet SCSI ed indica l'estensione del protocollo di accesso SCSI (Small Computer System Interface) alle reti TCP/IP.

	ACCESSO IN RETE	MEZZO TRASMISSIVO	PROTOCOLLO DI I/O	CONDIVISIONE DEI DATI
DAS	no	dipende dall'elaboratore: rame, cavo parallelo, cavo SCSI, fibra…	SCSI	no
SAN	si	il mezzo più comune è la fibra ottica	SCSI (FCP)	si, con software specializzato
NAS	si	Ethernet	NFS, CIFS	si
iSCSI	si	Ethernet	SCSI	si, con software specializzato

Tabella 18 - Confronto tra i metodi di connessione dei dispositivi di memorizzazione

5.3.2 LE STORAGE AREA NETWORK

Una *Storage Area Network* (SAN) è, come si è visto, una rete di trasmissione dati dedicata ai dispositivi di memorizzazione. Le realizzazioni correnti utilizzano una rete in fibra ottica, ma il concetto di SAN è indipendente dal mezzo trasmissivo utilizzato.
L'accesso alla memoria da parte delle applicazioni avviene attraverso comandi di I/O (block I/O) che, come nei sistemi tradizionali, identificano lo specifico dispositivo (nastro o disco) e, nel caso di dischi, la localizzazione del dato (settore).
Le SAN si sono diffuse soprattutto per le seguenti caratteristiche:

- prestazioni: in confronto ai tradizionali sistemi SCSI, i sistemi SAN consentono maggiori distanze tra gli elaboratori ed i sistemi di memorizzazione, maggiore disponibilità e prestazioni più elevate;
- consolidamento: con questo termine si intende la capacità di sostituire un complesso di sistemi eterogenei e non integrati con un numero limitato di dispositivi condivisi da tutte le applicazioni. I sistemi SAN realizzano il consolidamento dei sistemi di memorizzazione, in quanto consentono la condivisione di grosse quantità di dati anche tra elaboratori posti a notevole distanza ed inoltre disaccoppiano le applicazioni dalle specifiche tecniche di memorizzazione.

In una SAN, dispositivi con caratteristiche diverse possono essere combinati in modo da formare un'unica struttura di memorizzazione (*disk array*) condivisa da più server. Questa struttura offre di solito le funzioni tipiche dei sistemi di memorizzazione avanzati quali: la ridondanza delle registrazioni (RAID[60]), la replica speculare remota (*remote mirroring*) e funzioni di replica istantanea. La struttura di memorizzazione può essere partizionata in modo da riservare a ciascun server una porzione dello spazio disco disponibile.
Lo spazio disponibile in una SAN può essere gestito da un unico punto di controllo. Di norma le funzioni di controllo includono la possibilità di definire le relazioni tra gli elaboratori e le porzioni di memoria disco con tecniche chiamate *zoning e LUN*[61] *masking*.
Le tecniche di *zoning* consistono nella segmentazione dello spazio disco in zone dedicate a gruppi di utenti e non accessibili da utenti esterni[62].

[60] L'acronimo RAID significa *Redundant Array of Independent (o Inexpensive) Disks* ed indica sistemi di memorizzazione che registrano le informazioni in modo ridondato su più dischi per aumentare l'affidabilità del dispositivo.

[61] Il termine LUN (Logical Unit Number) è stato originariamente introdotto per indirizzare le unità di registrazione in un dispositivo SCSI.

[62] Le funzioni di zoning possono essere realizzate sia via hardware, sfruttando le caratteristiche degli switch, sia via software.

Attraverso il mascheramento delle unità logiche (*LUN masking*) è invece possibile abilitare o inibire l'accesso allo spazio disco condiviso secondo regole che assicurano il corretto utilizzo della memoria condivisa.

5.3.3 Le tecniche per la virtualizzazione

Fin dagli anni '80 si è sentita l'esigenza di gestire il patrimonio informativo in modo unitario, rendendo le applicazioni indipendenti dalla localizzazione fisica dei dati.
Le *Storage Area Network* realizzano parzialmente questa indipendenza, consentendo di gestire lo spazio disco come una entità logica indipendente dalla localizzazione effettiva dei dati, pur mantenendo il legame tra applicazione e dispositivo logico.
Lo sviluppo tecnologico consente oggi di realizzare il disaccoppiamento pressoché totale tra le applicazioni ed il patrimonio informativo delle amministrazioni: le tecniche che realizzano questa indipendenza prendono il nome di virtualizzazione delle informazioni.
La virtualizzazione delle informazioni ha molti vantaggi in termini di mantenibilità del software, semplicità gestionale, sicurezza ed affidabilità.
Per quanto concerne la continuità operativa, la virtualizzazione migliora la capacità di operare in presenza di problemi circoscritti ed offre una notevole flessibilità nella progettazione di una soluzione di recupero. È infatti possibile modificare la distribuzione dei dati in funzione delle esigenze di recupero, senza che ciò abbia impatto sulle applicazioni. Inoltre, essendo le applicazioni svincolate dalle strutture dati, è possibile ripristinare i servizi "in emergenza" anche con basi informative ridotte.
La figura 19 illustra, a scopo esemplificativo, lo schema di una generica architettura per la virtualizzazione delle informazioni.
Secondo tale modello, il sistema di gestione dei dati aziendali si comporta come un fornitore di servizi verso le applicazioni, rappresenta cioè un'istanza di un'architettura di tipo orientato ai servizi (*Service Oriented Architecture*). Questo sistema è pertanto caratterizzato da interfacce standard (XML/SOAP, SQL/ODBC, ecc.) e deve poter interagire con diversi sistemi operativi.
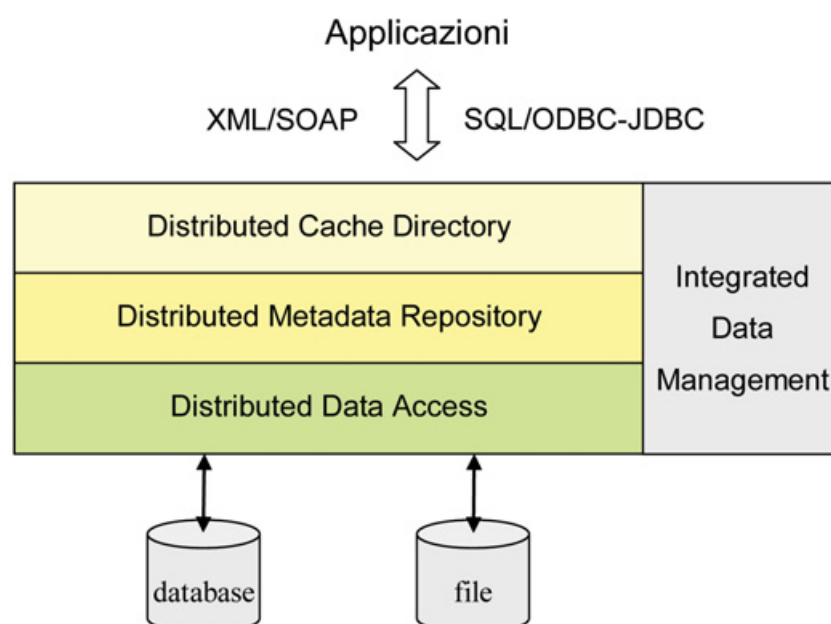
Figura 19 - Modello di virtualizzazione dei dati

Il componente *Distributed Cache Directory* assicura l'efficienza dell'accesso ai dati, prelevandoli dalla specifica area di transito (cache) in cui essi sono temporaneamente memorizzati. Tale componente realizza pertanto l'indipendenza delle applicazioni dai sistemi server che gestiscono i dati (NAS o SAN), nonché dalla loro dislocazione geografica.
Il *Distributed Metadata Repository* ha la funzione di integrare le informazioni presenti nelle diverse unità logiche di memorizzazione, fornendo alle applicazioni una vista unitaria dei dati. Questo componente ha anche la funzione di scegliere il percorso di accesso ottimale quando sono disponibili più repliche dei dati.
L'accesso ai diversi dispositivi di storage presenti nel sistema informatico è gestito dal *Distributed Data Access*, che deve essere in grado di interfacciare tutti i sistemi di memorizzazione presenti nell'organizzazione (unità nastro, file, database, ecc.).
I processi svolti dai componenti elencati sono coordinati dall'*Integrated Data Management*. Questo componente ha il compito di scegliere la strategia di accesso ai dati più opportuna in funzione delle esigenze di prestazioni, sicurezza e disponibilità.
Il modello appena descritto è teorico e non trova la totale rispondenza negli attuali prodotti di mercato. Tuttavia già oggi sono disponibili prodotti commerciali che realizzano parti significative del modello esposto, raggiungendo un elevato grado di disaccoppiamento tra applicazioni e dati.
Esistono inoltre altri modelli di virtualizzazione che prevedono una diversa suddivisione dei livelli, ma che comunque realizzano l'indipendenza delle applicazioni dai sistemi di storage attraverso la scomposizione delle funzioni di accesso ai dati in più componenti che corrispondono a livelli crescenti di astrazione delle informazioni.
A titolo di esempio si cita il modello proposto dall'associazione *Storage Networking Industry Association* (SNIA) che ha l'obiettivo di sviluppare modelli interoperabili di sistemi storage caratterizzati da efficienza ed affidabilità. Il documento di riferimento si può trovare all'indirizzo:

- http://www.snia.org/tech_activities/shared_storage_model/SNIA-SSM-text-2003-04-13.pdf

5.4 LE TECNOLOGIE PER IL SITO DI EMERGENZA

I piani di continuità operativa spesso prevedono la disponibilità di un sito attrezzato che possa essere utilizzato in caso di emergenza. Teoricamente in questo sito possono essere usate le stesse soluzioni informatiche del sito primario, ma in pratica spesso si preferisce utilizzare delle tecnologie che consentono di ridurre i costi.
Le caratteristiche ottimali della tecnologia dipendono dalla soluzione prescelta.
In soluzioni basate su accordi di assistenza volontaria (ad esempio mutuo soccorso) non ci si può basare su tecnologie che vincolerebbero significativamente le amministrazioni, ma occorre adottare un piano di continuità operativa flessibile accettando tempi di ripristino del servizio variabili tra qualche giorno ed una settimana.
Una soluzione tipica, soprattutto nel caso di accordi tra organizzazioni indipendenti, prevede che l'ente soccorritore renda disponibili i locali attrezzati e gli apparati ausiliari (alimentazione, LAN, router, PC, ecc.) mentre l'organizzazione in emergenza provvederà ad

acquisire i server necessari per ripristinare il servizio[63]. Questa soluzione è valida soprattutto quando il servizio può essere erogato con apparati che è possibile reperire facilmente[64] ed hanno configurazioni standard.
Quando si adottano soluzioni basate su risorse condivise, è possibile ricorrere a tecniche di virtualizzazione dei sistemi per fare in modo che su uno stesso apparato possano essere attivati, all'occorrenza, ambienti elaborativi eterogenei.
Si tratta di sistemi virtuali[65], o *Virtual Machine*, che permettono di emulare, su uno stesso elaboratore, più ambienti elaborativi indipendenti, ciascuno caratterizzato da un proprio sistema operativo ed una propria configurazione.
Una soluzione mista, che consente comunque una notevole riduzione dei costi, consiste nel ricorrere a risorse logistiche e strutturali condivise (locali, alimentazione, condizionamento, sorveglianza, ecc.) prevedendo invece risorse elaborative dedicate all'amministrazione in uno stato quiescente (*hot standby*).

5.4.1 Hot standby

Le soluzioni di questo tipo prevedono un ambiente elaborativo di riserva ad attivazione veloce con la capacità elaborativa necessaria per mettere in produzione l'applicazione da proteggere. I sistemi possono avere una capacità elaborativa inferiore a quella dei sistemi in esercizio, ma devono avere la stessa configurazione per fare in modo che le applicazioni possano operare correttamente in condizioni di emergenza. Peraltro alcune esperienze di casi reali di disastro hanno evidenziato la necessità di una potenza elaborativa nel centro di backup superiore a quella del centro di produzione, almeno nel primo periodo di gestione dell'emergenza (esempio: recupero del carico di lavoro accumulato a seguito del fermo).
L'allineamento delle configurazioni tra il sistema in esercizio ed il sistema in *hot standby* è un aspetto particolarmente critico, in quanto un disallineamento può compromettere l'efficacia della soluzione di continuità operativa[66]. Per facilitare l'allineamento delle configurazioni, sono disponibili prodotti che automaticamente propagano l'aggiornamento del software di base e delle configurazioni sui sistemi in *hot standby*.
Sono inoltre disponibili delle tecnologie che automatizzano la rilevazione dei disastri ed il recupero: se avviene un evento catastrofico sul sito primario, il sistema in standby si accorge automaticamente dell'accaduto e inizia il processo di recupero, incluso il riavvio dell'applicazione e l'abilitazione dell'accesso via rete agli utenti.

---

[63] Se l'amministrazione dispone dei salvataggi dei dati e degli ambienti elaborativi, una volta che si è recuperato l'hardware è possibile ristabilire la configurazione e riattivare il servizio in tempi accettabili (2-4 giorni).

[64] In molti casi i servizi principali possono essere erogati con server di classe PC che possono essere acquistati da fornitori in grado di consegnarli in brevissimo tempo.

[65] Tali sistemi esistono da tempo in ambiente legacy ma recentemente si stanno diffondendo anche sui più recenti sistemi operativi per la loro versatilità.

[66] Ciascuna variazione alla configurazione e ciascun aggiornamento dei sistemi di base presso il sito sistema primario dovrebbe essere riportata sui sistemi in hot standby, ma può capitare che per motivi diversi (ritardi, differente comportamento dell'hardware, errori operativi, ecc.) si crei comunque un disallineamento che può inficiare la corretta esecuzione delle applicazioni. Il modo migliore per evitare che questi problemi emergano solo nel momento dell'emergenza è eseguire prove periodiche.

Nel progettare la soluzione occorre prevedere il collegamento della periferia al sito di recupero, bisogna inoltre individuare la modalità di attivazione della connessione ai sistemi in standby in caso di necessità. Sono possibili due modalità:

- i sistemi periferici vengono configurati in modo da connettersi al sito di emergenza invece del sito primario, attivando eventualmente una procedura di emergenza;
- la rete viene riconfigurata in modo da indirizzare le connessioni della periferia verso il sito di emergenza.

La prima soluzione è di realizzazione più semplice[67], ma comporta la necessità di intervenire presso la periferia e ciò allunga inevitabilmente i tempi di ripartenza.
La riconfigurazione della rete consente tempi di ripartenza inferiori, soprattutto se questa avviene in modo automatico a seguito di un evento associato al rilevamento del disastro. Tale soluzione comporta però il coinvolgimento del gestore della rete ed è quindi condizionata dalla tipologia di servizi che questi offre.

5.4.2 Il cluster remoto

Per ridurre ulteriormente i valori di RTO e RPO è possibile ricorrere a tecniche come il clustering remoto (*wide area clustering*), in cui presso più siti sono attivi più sistemi che operano in modo concorrente (gli utenti si connettono al sito più vicino oppure meno usato).
La tecnologia del cluster è spesso utilizzata per aumentare l'affidabilità dei sistemi elaborativi: due o più sistemi condividono la stessa base informativa ed in condizioni ordinarie operano in modo da rendere massime le prestazioni (ad esempio bilanciando il carico) mentre nel caso di panne di un sistema tutto il carico sarà assorbito dal sistema rimasto attivo. Poiché i due sistemi devono operare in stretto sincronismo, normalmente vengono connessi con un canale ad elevata capacità trasmissiva.
Se si utilizza questa soluzione rendendo remoti i due sistemi in cluster, è possibile fare in modo che, nel caso un evento blocchi un sito, l'intero carico elaborativo possa essere sostenuto dal sistema in cluster rimasto attivo.
Affinché questa tecnologia possa essere utilizzata ai fini della continuità operativa, è necessario che presso ciascuno dei due siti sia presente una replica dei dati correntemente utilizzati dall'altro sito. Tale replica può ottenersi con le tecniche di replica descritte in precedenza (ad esempio *mirroring* dei dati).
Una soluzione di questo tipo ha il vantaggio di avere tempi di ripartenza ridottissimi, purché tutti i dati occorrenti siano presenti presso il sito di recupero. Inoltre è necessario che i due sistemi siano collegati con un canale ad alta velocità ed elevata disponibilità (normalmente canale in fibra ottica): ciò rende la soluzione costosa, soprattutto se il sito di recupero dista parecchio dal sito primario.
Il mercato rende oggi disponibili diverse soluzioni per il cluster remoto dei sistemi che si differenziano negli aspetti di dettaglio (modalità di collegamento dei sistemi, modalità di replica dei dati, caratteristiche degli automatismi per il passaggio alle condizioni di emergenza, integrazione con altri sistemi di recovery, ecc.).
Il cluster remoto è la soluzione di continuità operativa che offre la maggiore flessibilità d'uso, in quanto consente di distribuire il carico tra i sistemi in cluster in funzione delle specifiche esigenze di prestazioni, manutenzione o recupero di condizioni di emergenza.

[67] Dal punto di vista tecnico è sufficiente attivare una procedura che modifichi gli indirizzi relativi al sito in condizioni di fermo.

Appendici

Appendice A: Indice tipo per il documento di BIA

L'indice del documento prodotto al termine della BIA può essere strutturato come di seguito:

- Premessa
  - Identificazione delle esigenze generali di continuità operativa
  - Partecipanti alla fase di Business Impact Analysis
- La fase di Business Impact Analysis
  - Obiettivi
  - Approccio adottato
- Caratterizzazione dei servizi dell'amministrazione
  - La struttura dei servizi
  - Analisi di criticità e di impatto dei servizi
  - Obiettivi di ripristino
- Caratterizzazione dei sistemi informatici
  - Architettura applicativa
  - Architettura tecnologica
- Identificazione delle esigenze di continuità operativa dei sistemi informatici
  - Associazione dei sistemi informatici ai servizi
  - Identificazione del perimetro di intervento
- Priorità di intervento

Nel seguito sono descritti i contenuti dei principali capitoli.

Premessa

Il capitolo ha come scopo quello di illustrare e motivare le scelte di base dell'amministrazione riguardo alle esigenze di continuità operativa[68], con riferimento al contesto istituzionale e normativo in cui si trova ad operare. La premessa fornisce indicazioni sui procedimenti che l'amministrazione intende prendere in esame in termini di continuità operativa, motivando tali indicazioni e riservando a una fase successiva il riesame e l'eventuale allargamento dell'indagine.

[68] Ad esempio, le aree prioritarie (in termini di procedimenti o sottosistemi informatici) sulle quali l'amministrazione intende intervenire nel breve periodo.

In questo capitolo sono anche presentati i ruoli e le organizzazioni interne all'amministrazione che hanno preso parte alla stesura del documento.

LA FASE DI BUSINESS IMPACT ANALYSIS

Questo capitolo contiene le informazioni relative agli obiettivi dello studio e all'approccio adottato.
Gli obiettivi tipici sono quelli già citati, ovvero:

- la delimitazione del perimetro, sia in termini di servizi che in termini di "isole" informatiche;
- la valutazione dell'impatto della non disponibilità dei servizi;
- la valutazione degli obiettivi di ripristino richiesti;
- la definizione delle priorità degli interventi.

Quanto all'approccio, nel capitolo devono essere fornite le seguenti indicazioni minime:

- livello di dettaglio dell'analisi;
- modalità di raccolta e di validazione delle informazioni, sia relativamente ai servizi che relativamente alle risorse informatiche;
- modalità e regole di classificazione dei servizi per criticità (ad es. sulla base del livello qualitativo di rilevanza operativa e strategica del servizio in esame);
- modalità di attribuzione della vulnerabilità alle risorse informatiche;
- composizione della griglia di valutazione della criticità delle risorse informatiche e dei conseguenti impatti;
- modalità di individuazione degli obiettivi di ripristino;
- approccio alla valutazione (qualitativo, quantitativo).

CARATTERIZZAZIONE DEI SERVIZI DELL'AMMINISTRAZIONE

Questo capitolo illustra la struttura delle attività dell'amministrazione organizzate in servizi. Il modello descrittivo che viene costituito è la base di riferimento sulla quale sono mappate le risorse informatiche, così da poter individuare il livello di criticità delle risorse stesse in funzione del servizio da queste implementato: le risorse informatiche ereditano gli obiettivi di continuità operativa dalle esigenze di continuità dei servizi cui afferiscono[69].
Per rendere più semplice il lavoro, è utile raggruppare più servizi in classi, ad esempio nei casi in cui un unico sottosistema informatico (e quindi un insieme di risorse ben circoscritto) supporti più servizi. Più in generale, si ricordi che l'analisi è finalizzata alla continuità operativa: per questo motivo, il modello descrittivo dei servizi potrebbe essere parziale, e non rispecchiare necessariamente in modo dettagliato la totalità delle attività dell'amministrazione e le relazioni reciproche tra queste.

[69] Nel caso di risorse che supportino più servizi, ereditano le esigenze del servizio più critico tra quelli supportati.

Per ognuno dei sottosistemi informatici individuati devono essere indicati i requisiti di ripristino nel caso di emergenza. I requisiti di ripristino generalmente sono espressi in termini dimensionali temporali, tramiti gli indicatori RTO (*Recovery Time Objective*) e RPO (*Recovery Point Objective*). Vengono definiti RTO e RPO per i singoli servizi dell'amministrazione, e quindi per le risorse informatiche che supportano i servizi stessi.
In genere, i valori di RTO ed RPO vengono normalizzati e raggruppati per tipologia di intervento, in modo da non diversificare troppo le soluzioni di continuità da implementare.

CARATTERIZZAZIONE DEI SISTEMI INFORMATICI

Questo capitolo contiene informazioni sui sistemi informatici essenziali al mantenimento dei servizi critici. Il livello di dettaglio da utilizzare è naturalmente finalizzato agli scopi della continuità operativa. Oltre ai sistemi informatici rilevati nella fase di caratterizzazione dei procedimenti dell'amministrazione, si dovranno aggiungere i sistemi informatici che vi si interfacciano (in particolare i sistemi "alimentanti" eventualmente anche esterni all'amministrazione) ed eventuali risorse informatiche che – per questione di vincoli tecnologici in essere – dovesse essere necessario inserire nel perimetro.
La caratterizzazione dei sistemi informatici deve consentire almeno di individuare:

- le dipendenze funzionali tra sottosistemi informatici (in modo da poter isolare in modo consistente eventuali aree di intervento);
- le tecnologie presenti e gli eventuali vincoli che pongono (propedeutici alla definizione delle soluzioni di continuità)

Per quanto attiene la rappresentazione e la descrizione dei sistemi informatici, ovvero delle architetture applicative e tecnologiche, l'amministrazione adotterà i propri standard documentali ICT. È in generale utile produrre sia un documento testuale, sia un documento di tipo grafico schematico.
La caratterizzazione delle risorse informatiche deve essere curata in termini di connettività fisica e di interfacce applicative; non è necessario, invece, rilevare i dettagli di configurazione delle singole risorse.

IDENTIFICAZIONE DELLE ESIGENZE DI CONTINUITÀ DEI SISTEMI INFORMATICI

Con riferimento ai requisiti di ripristino dei servizi già individuati, in questo capitolo vengono analizzati i seguenti due aspetti:

- associazione dei sistemi informatici ai servizi;
- identificazione del perimetro di intervento nell'ambito del sistema informatico.

PRIORITÀ DI INTERVENTO

In questo capitolo vanno elencate le priorità di intervento, individuate sulla base delle esigenze di continuità, della vulnerabilità delle risorse e delle criticità dei servizi da proteggere.

Appendice B: Indice tipo per il Piano di continuità operativa

Nel seguito viene presentato, a titolo di esempio, l'indice e la struttura di un possibile piano di continuità operativa.
Indice

- Sezione introduttiva
  - Valutazioni BIA
  - Valutazioni Risk Assessment
  - Strategie di ripristino selezionate
- Quadro operativo
- Fase di notifica e attivazione
  - Procedure di notifica e attivazione
  - Valutazione del danno
- Fase di ripristino
  - Sequenza delle azioni di ripristino
  - Procedure di ripristino
- Fase di rientro alla condizione iniziale
- Appendici
  - Business Impact Analysis
  - Risk Assessment
  - Sistema informatico nel perimetro del Piano
  - Strategie di ripristino
  - Risultati delle simulazioni

Nei paragrafi che seguono sono descritti i contenuti delle sezioni di questo indice.

Sezione introduttiva

Questa sezione vuole orientare il lettore sulla tipologia e la collocazione delle informazioni contenute nel Piano. In essa viene fornito:

- un quadro di insieme del contesto, arricchito da elementi informativi per facilitare sia la lettura del Piano che la sua manutenzione ed evoluzione;
- i dettagli per comprendere l'applicabilità dei contenuti, prendere decisioni su come utilizzare il Piano e indicare gli eventuali collegamenti con altri piani e, più in gene-

rale, con documenti rilevanti per il processo globale di gestione della continuità operativa.

Più in dettaglio, tra le informazioni contenute nella sezione introduttiva, il lettore potrà trovare:

- la finalità del Piano, vale a dire il motivo dello sviluppo del Piano stesso e i suoi obiettivi;
- la descrizione della/le organizzazione/i impattate dal Piano;
- l'indicazione di tutti i documenti che riferiscono o sono riferiti dal Piano;
- il perimetro di riferimento del Piano, sia in termini di sistemi oggetto di ripristino che in termini di eventi da prendere in considerazione (ad esempio: il presente Piano non è applicabile ai casi in cui l'assenza di operatività del servizio A è inferiore alle 3 ore; il presente piano è applicabile a emergenze di tipo ambientale, ma non a casi di distruzione totale del CED);
- i vincoli e le eventuali dipendenze dell'amministrazione da organizzazioni esterne (erogatore di energia elettrica, altre amministrazioni, ecc.);
- le referenze (riferimenti delle altre organizzazioni verso cui esistono vincoli e/o dipendenze);
- il registro delle modifiche occorse in fase di rivisitazione del Piano.

Quadro operativo

Questa sezione contiene dettagli riguardanti il sistema oggetto del Piano. Di esso devono essere riportati i seguenti elementi:

- Una descrizione generale delle "isole IT" da proteggere, che includa l'architettura fisica e logica, gli eventuali siti su cui il sistema è distribuito, le modalità di connessione, i meccanismi di memorizzazione dei dati, il traffico. È utile un disegno dell'architettura che includa i dispositivi di sicurezza (e.g., firewall, connessioni interne/esterne).
- La linea di successione, cioè la catena di escalation che deve essere adottata nel caso in cui, al momento dell'attivazione del Piano, una o più persone preposte non sia disponibile o non sia in grado di operare secondo il Piano.
- Ruoli, responsabilità, gerarchia e meccanismi di coordinamento previsti.
- Attività assegnate ai vari ruoli e gruppi. Come anticipato al paragrafo 1.3.1, è consigliabile indicare ruoli e non persone, in modo da non richiedere modifiche del Piano per far fronte al turn-over del personale.

Fase di notifica e attivazione

In questa sezione del Piano vengono definite le azioni da svolgere nel momento in cui si registra e/o quando si prevede che stia per verificarsi un'emergenza (allertare il personale preposto, stabilire il danno al sistema, decidere se attivare il proseguo del Piano).

Procedure di notifica e attivazione

Un'emergenza può verificarsi con o senza preavviso: le procedure di notifica e attivazione devono poter gestire entrambi i casi e dovrebbero garantire la notifica al personale addetto al ripristino in qualunque momento si renda necessario, sia durante l'orario di lavoro che fuori[70].
Il primo gruppo da attivare è quello preposto alla valutazione del danno. A seguito del lavoro di questo gruppo, il Piano indicherà i successivi gruppi da attivare.
Le notifiche possono essere realizzate attraverso telefonate, e-mail, comunicazioni di persona. Gli strumenti più efficaci sono la radio, la televisione e il web, mentre sono meno efficaci le notifiche tramite e-mail, non essendoci garanzia del buon esito dell'operazione e dell'effettiva lettura del messaggio. Se il Piano prevede che le notifiche possano essere fatte con questo sistema, è necessario sensibilizzare il personale coinvolto sulla necessità di leggere assai frequentemente la propria posta elettronica.
Le procedure definite devono contemplare i casi in cui non sia possibile contattare il personale previsto. Una tecnica spesso utilizzata è il cosiddetto "albero delle chiamate": si assegnano precisi doveri a determinate persone [ruoli] che assumono la responsabilità di avvisarne altre. Per ogni persona da avvisare, deve essere definita l'azione alternativa da intraprendere se non è possibile contattarla.
La lista delle persone da contattare deve essere rivista e aggiornata frequentemente, e deve contenere tutte le informazioni utili per il contatto. Ecco, nel seguito, un esempio di informazioni relative a una persona della lista:

Team di Software di Sistema
Team Leader—Necessario
XXX XXXX
Via XXXX X, XXX
Casa : (+39) (0)XX-XXX-XXXXXX
Ufficio: (+39) (0)XX-XXX-XXXXXX
Cell: +39-XXX-XXXXX
E-mail: XXX@azienda.com

Nella lista devono essere presenti anche i riferimenti di organizzazioni esterne o di partner (per esempio i fornitori) che devono essere informati tempestivamente dell'emergenza: in certi casi, infatti, i partner possono avere precise responsabilità nella gestione dell'emergenza, per cui la mancata notifica inficia le eventuali rivalse da parte dell'amministrazione per inadempienze.
Un ruolo particolare che deve essere definito nel Piano è quello del "coordinatore" del Piano stesso, responsabile del suo corretto svolgimento. Il coordinatore deve essere indicato chiaramente e in modo univoco (sebbene anche nel suo caso valga la regola di indicare un sostituto che gli subentri in caso di indisponibilità).

Valutazione del danno

Per determinare le dimensioni e il perimetro dell'intervento necessario a fronte di un'emergenza, è necessario individuare la natura e l'estensione del danno subito dall'ammini-

[70] Ciò spesso comporta la necessità di accordi sindacali specifici.

strazione. Nel rispetto della sicurezza fisica delle persone che devono valutare il danno, quanto prima si riesce a completare la valutazione, tanto prima si riesce a operare per gestire la situazione e avviare il ripristino dell'operatività.
Nella stesura del Piano, si stabiliranno quali informazioni devono essere raccolte e si fisseranno i tempi massimi per la loro raccolta. Le principali informazioni da raccogliere nel corso della valutazione sono, generalmente:

- natura dell'emergenza che si è verificata;
- presenza di morti o feriti;
- probabilità che si verifichi un'ulteriore emergenza o che questa peggiori la sua natura causando un danno maggiore;
- area in emergenza;
- stato dell'infrastruttura fisica (integrità strutturale del CED, presenza di energia elettrica, funzionamento delle comunicazioni, stato dell'impianto di condizionamento, ecc.);
- inventario e stato funzionale della strumentazione IT (parzialmente funzionante, completamente non funzionante);
- tipo di danno alla strumentazione IT o ai dati (rottura, allagamento, incendio, sovralimentazione, ecc.);
- componenti da sostituire;
- tempo stimato per il ripristino dell'operatività in loco.

Il Piano dovrà inoltre stabilire se e quando deve essere compiuta una successiva valutazione della situazione (ad esempio a valle dell'attivazione delle prime contromisure previste).
Tutte le azioni successive previste dal Piano verranno effettivamente attivate se e solo se la valutazione del danno indica che c'è necessità di farlo.
In altre parole, se i danni non inficiano l'operatività in modo grave (il termine "grave" va quantificato secondo quanto stabilito dall'analisi di impatto e da eventuali livelli di servizio attesi), le azioni previste dal Piano non vanno attivate. Invece, se almeno uno dei criteri di attivazione del Piano si verifica, le azioni vanno attivate.
I criteri di attivazione devono essere determinati in modo univoco e inseriti nel Piano. I criteri generalmente riguardano:

- la sicurezza del personale e l'estensione del danno alle strutture;
- la dimensione del danno ai beni informatici (fisico, operativo, economico);
- l'impossibilità di garantire la missione dell'amministrazione.

FASE DI RIPRISTINO

Le operazioni di ripristino iniziano dopo la valutazione del danno, l'avvenuta notifica al personale preposto e la mobilitazione dei gruppi di lavoro secondo la strategia individuata da chi ha la responsabilità del coordinamento (il coordinatore del Piano, di cui si è già parlato).

La fase di ripristino comprende tutte le azioni da eseguire per assicurare la ripresa dell'operatività del sistema nella condizione temporanea, per sanare i danni nel sito/sistema danneggiato e tornare alla situazione al momento prima del verificarsi dell'emergenza, ripristinando l'operatività nel sito originario o in un sito alternativo.
A conclusione della fase di ripristino, il sistema sarà in grado di operare come definito nel Piano: dipendentemente dalla strategia di ripristino adottata, si può prevedere di implementare alcuni processi in modo manuale, ripristinare l'operatività su un altro sito o ricollocare il tutto in un nuovo sito.
Il gruppo che ha la responsabilità del ripristino deve essere in grado di eseguire tutte le attività previste in ogni caso, anche se non fosse stato possibile eseguire le fasi precedenti del Piano. In altre parole, il gruppo di ripristino non deve aspettare alcun input di tipo "bloccante" dalle attività precedenti: tutto ciò che deve fare è già scritto sul Piano, non deve far altro che eseguirlo.
Si noti che il Piano deve prevedere anche situazioni in cui l'emergenza abbia prodotto solo danni parziali e circoscritti nell'ambito dell'amministrazione. In questi casi, il Piano deve prospettare una condizione di lavoro organizzata in "due flussi": nel primo flusso, le attività proseguono ordinariamente nelle aree non toccate dall'emergenza; nel secondo flusso, ci si concentra nella reazione al verificarsi dell'emergenza e alle attività di ripristino.

SEQUENZA DELLE AZIONI DI RIPRISTINO

Le procedure di ripristino devono riflettere le priorità definite nella BIA. La successione delle attività è perciò determinata dai tempi di ripristino fissati per i vari servizi critici.
È preferibile che le procedure siano dettagliate e descritte come sequenze di passi, il che contribuisce a garantire che le risorse che concorrono all'erogazione di un determinato servizio siano ripristinate nel modo logicamente corretto e che i dati siano mantenuti in modo coerente (senza squadrature).
Ad esempio, se il servizio è distribuito, è necessario ripristinare la LAN e, successivamente, i sistemi attestati su di essa, poi le applicazioni e il data server. Nel caso di servizi con un elevato livello di sicurezza, prima dell'applicazione specifica andranno ripristinati i componenti di sicurezza. E così via.
Nel caso di ripristino del sistema in un sito alternativo, è necessario assicurarsi della disponibilità di tutti gli elementi necessari (hardware, software, dati). Le procedure di trasferimento e/o aggiornamento di tali elementi sono parte essenziale del processo, e devono essere definite in modo coerente con le attività di gestione ordinaria del sistema (vale a dire, devono impattare il meno possibile su queste ultime).
Per quanto riguarda la disponibilità delle risorse umane necessarie a garantire l'operatività nel sito secondario, si può pensare a definire in modo preventivo tutte le eventuali approvazioni richieste per autorizzare, per esempio, i viaggi, la disponibilità di badge di accesso, l'acquisto di materiale di consumo ecc...

PROCEDURE DI RIPRISTINO

Per rendere il più efficiente possibile la fase di esecuzione delle attività di ripristino, il Piano deve contenere procedure specifiche per il sistema considerato. Non è possibile dunque anticipare i possibili contenuti, che dipendono dal singolo caso in esame. È pos-

sibile tuttavia indicare alcune procedure "tipiche", che vengono elencate nel seguito a mero titolo di esempio:

- ottenimento delle autorizzazioni di accesso ai beni o a alle zone danneggiate;
- notifica alle altre amministrazioni ed entità esterne che possono essere impattate dalla non disponibilità dei servizi;
- ottenimento dei necessari posti di lavoro opportunamente configurati;
- ottenimento e installazione delle risorse hardware necessarie;
- ottenimento e caricamento dei supporti utilizzati per la protezione dei dati;
- ripristino dei sistemi critici e relativi software applicativi;
- ripristino dei dati;
- collaudo delle funzionalità, inclusi i controlli di sicurezza;
- connessione dei sistemi alle reti o ad altri sistemi esterni;
- verifica della corretta operatività degli apparati alternativi.

Le procedure di ripristino vanno scritte in modo molto semplice, diretto, preferibilmente come sequenze di passi: è decisamente sconsigliabile la presenza di attività non procedurali.
Il modo ideale per definire le procedure da seguire è senz'altro la stesura di check-list, anche per gli aspetti relativi a errori che possono verificarsi e a percorsi alternativi da seguire in particolari situazioni.

FASE DI RIENTRO ALLA CONDIZIONE INIZIALE

In questa fase le attività di ripristino sono terminate e l'operatività ritorna alla situazione originaria (standard). Questa sezione del Piano descrive appunto tutte le operazioni da eseguire per effettuare il rientro dell'operatività.
Se il sito primario non è più agibile, le operazioni descritte in questa sezione del Piano possono essere utilizzate per realizzare un nuovo sito, gemello di quello originario.
La fase di ricostituzione del sito primario è di responsabilità di un gruppo ben individuato, descritto e referenziato nel Piano. È buona pratica definire il gruppo di lavoro comprendendo professionalità tali da essere in grado di realizzare le attività necessarie anche in presenza di documentazione parziale o assente.
Anche in questo caso, è possibile indicare, a titolo di esempio, le operazioni e le procedure che generalmente sono descritte in questa sezione del documento (presentate nell'ordine temporale in cui normalmente devono essere eseguite):

- ripristino del supporto all'infrastruttura (energia elettrica, acqua, sicurezza, controlli ambientali, ecc.);
- installazione hardware, software, firmware;
- ripristino della connettività e delle interfacce con gli apparati di rete e sistemi esterni;
- test/verifica della piena funzionalità del sistema;
- restore dei dati operazionali a partire dai backup;

- spegnimento del sistema alternativo (di emergenza);
- rimozione/riallocazione dei materiali di consumo utilizzati per il sito alternativo;
- rientro del personale alla normale operatività.

Appendici

Le appendici devono contenere tutte le informazioni utili e a supporto del piano, sia in termini di comprensione sia in termini di fruibilità. Possono costituire appendice del piano i seguenti documenti:

- Business Impact Analysis;
- Risk Assessment;
- Descrizione del sistema informatico nel perimetro del Piano;
- strategie di ripristino;
- risultati delle simulazioni;
- contatti interni;
- contatti fornitori;
- livelli di servizio;
- procedure operative IT standard;
- piano di evacuazione.

Appendice C: Modello di protocollo di intesa

Modello di protocollo di intesa per la progettazione, acquisizione e gestione comune di un centro di continuità operativa

TRA

AMM1, con sede in .... via .... nella persona di ....

AMM2 ...

AMM3 ...

......

......

premesso e considerato che:

la salvaguardia dei sistemi informativi e la disponibilità dei servizi IT erogati al cittadino sono ormai una esigenza comune a tutte le amministrazioni pubbliche non più rinviabile, poiché la dipendenza di tali servizi dall'Information Technology è tale da compromettere l'operatività nel caso di indisponibilità dei sistemi;

l'elevato costo in termini economici necessario a implementare soluzioni di continuità operativa ha indotto le Amministrazioni sopra indicate ad avviare un'iniziativa finalizzata a realizzare servizi comuni, realizzando altresì le necessarie economie di scala e standardizzando soluzioni e procedure;

le sopra indicate Amministrazioni ritengono necessari per i propri sistemi di elaborazione, in coerenza con le esigenze di protezione da disastro informatico, di tutelare i propri patrimoni informativi e di incrementare la disponibilità dei servizi erogati mediante la progettazione, l'acquisizione e la realizzazione di un centro di elaborazione comune, interconnesso ai siti primari, in grado di garantire la Continuità Operativa nell'eventualità che i servizi erogati dal centro primario si rendano totalmente, o anche solo parzialmente, indisponibili a causa di eventi disastrosi o malfunzionamenti.

La soluzione, che si prevede sia attivata entro il 20XX, permetterà alle Amministrazioni di avere la disponibilità, presso terzi, di spazi adibiti a sala CED, nei quali ospitare i sistemi di elaborazione e i relativi sottosistemi, con attigue sale di controllo per il servizio di conduzione dei sistemi stessi. Tali sistemi saranno dimensionati per sostenere la replica dei dati (a disco e a nastro) con il sito primario e la rapida riattivazione delle applicazioni di produzione secondo elevati livelli di servizio;

VISTE le "Linee Guida del Governo per lo Sviluppo della Società dell'Informazione" emanate dal Ministro per l'innovazione e le tecnologie;

VISTA la direttiva del 16 gennaio 2002, "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali" emanata dal Ministro per l'innovazione e le tecnologie;

VISTO l'art. 15 della legge 7 agosto 1990, n. 241 che prevede che le amministrazioni pubbliche possano concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune;

VISTO il DPCM 6 agosto 1997, n. 452;

VISTO il decreto legislativo 7 marzo 2005, n. 82 recante "Codice dell'amministrazione digitale";

VISTA la delibera [segue lista delle Amministrazioni che sottoscrivono il protocollo]

AMM1

AMM2

AMM3

...

si conviene quanto segue:

Art. 1
Glossario e Acronimi

Ai fini del presente protocollo si intende per:

- CO – Continuità Operativa: insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il Disaster Recovery;
- CdC: Comitato di Coordinamento;
- CT: Comitato Tecnico;
- Disaster Recovery: insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso;
- Impresa: il soggetto, o i soggetti, incaricato(i) della realizzazione del Progetto;
- Outsourcing: attività svolta da soggetto esterno a favore di un'Amministrazione;
- Progetto: il progetto per la realizzazione del centro di continuità comune alle Amministrazioni sottoscriventi il presente Protocollo.

Art. 2
Oggetto del protocollo di intesa

Con il presente protocollo le parti si impegnano a procedere alla acquisizione dei servizi di cui all'art. 4 ed alla successiva realizzazione di un Centro di Continuità Operativa dedicato alle Amministrazioni sottoscriventi il presente Protocollo medesimo.

La firma del presente Protocollo d'intesa costituisce impegno per le amministrazioni aderenti a favorire la realizzazione del Progetto. Con successivi atti e tramite la stipula di appositi contratti con l'Impresa, ciascuna amministrazione procederà alla realizzazione del Centro di Continuità Operativa.

ART. 3
Obiettivi del Protocollo di intesa

Con la sottoscrizione del Protocollo, le parti intendono perseguire i seguenti obiettivi:

- dotare le Amministrazioni partecipanti di soluzioni di continuità e/o ripristino per i servizi ICT più critici;
- realizzare economie di scala e organizzative, condividendo servizi e risorse;
- standardizzare le metodologie nel campo della disponibilità dei sistemi ICT.

ART. 4
Fasi del Progetto

Il Progetto si articola nelle seguenti fasi (n.d.r.: a seconda dei casi concreti, non necessariamente in sequenza e non necessariamente tutte presenti nel Progetto):

1. progettazione operativa della soluzione (sempre presente);
2. messa a disposizione di spazi informatici attrezzati e gestiti e dei relativi servizi di logistica e sorveglianza;
3. erogazione dei servizi di risorse elaborative;
4. erogazione dei servizi di manutenzione delle risorse elaborative, nel rispetto degli eventuali diritti di terzi (n.d.r.: eventualmente anche quelle di proprietà dell'amministrazione);
5. erogazione dei servizi di assistenza operativa post-realizzazione della soluzione;
6. i servizi di cui sopra verranno definiti nel capitolato tecnico (successivo art. 5), anche sulla base di quanto indicato dall'art. 3 del DPCM 6 agosto 1997, n. 452.

ART. 5
Articolazione della struttura organizzativa

1. Il Comitato di Coordinamento (CdC)

Svolge le funzioni di indirizzo, governo, monitoraggio e controllo dello sviluppo e avvio del Progetto. È composto da [NUMERO] componenti effettivi e [NUMERO] componenti supplenti indicati nelle persone di:

- Componenti effettivi:
  XXX, nominato dal [AMM1], al quale spetta la funzione di Coordinatore del CdC;

YYY, nominato dal [AMM2];
ZZZ, nominato dal [AMM3];
....

- Componenti supplenti:
XXX1, nominato dal [AMM1];
YYY1, nominato dal [AMM2];
ZZZ1, nominato dal [AMM3];
...

In caso di impedimento di un componente effettivo a partecipare ad una riunione, quest'ultimo è sostituito, nelle funzioni allo stesso spettanti, dal componente supplente nominato dal medesimo soggetto che ha nominato il membro effettivo impedito a partecipare.
Il CdC è validamente costituito con la presenza di tutti i suoi componenti.
Il CdC si riunisce su convocazione del Coordinatore inviata, tramite lettera o fax o e-mail, a tutti i componenti almeno tre giorni lavorativi prima della data fissata per la riunione.
Il CdC si riunisce almeno su base mensile per tutta la durata delle attività previste dal Progetto. Di ogni riunione si redige il relativo verbale. Le deliberazioni del CdC sono assunte all'unanimità.

2. Compiti del CdC

Il CdC ha i seguenti compiti:

- entro un mese dalla sottoscrizione del presente Protocollo, definizione del piano di dettaglio delle proprie attività;
- entro tre mesi dalla sottoscrizione del presente Protocollo, definizione delle modalità amministrative e giuridiche di realizzazione del Progetto;
- entro quattro mesi dalla sottoscrizione del presente Protocollo, valutazione delle proposte realizzative sottoposte dal Comitato Tecnico di cui al successivo punto 3, inclusa la definizione dei costi di massima per la realizzazione del progetto;
- coordinamento e supervisione, con il supporto del CT, di tutte le attività concordate tra le Amministrazioni aderenti per la realizzazione del Progetto, per l'acquisizione dei beni e servizi necessari alla costituzione del centro comune di CO e alla gestione di quest'ultimo.

Il CdC è altresì incaricato di avviare tutte le altre iniziative che lo stesso riterrà opportune per favorire la realizzazione del Progetto.

3. Il Comitato Tecnico (CT)

Il Comitato Tecnico svolge la funzione di indirizzo tecnico nella realizzazione del Progetto In particolare:

- predispone le proposte tecniche per la realizzazione del Progetto; in particolare, predispone gli atti di gara e il capitolato tecnico;
- supporta il CdC predisponendo quanto è necessario per la valutazione e il controllo di tutto il Progetto. Il presidente del CT assume le funzioni di Responsabile di

Progetto, costituendo il tramite tra il Comitato stesso e l'Impresa che sarà incaricata della realizzazione del Progetto.

Il CT è composto da personale delle Amministrazioni partecipanti che abbia esperienza nella progettazione, realizzazione e gestione di Sistemi informatici. I componenti del CT sono:

- XXX2, nominato dal [AMM1], al quale spetta la carica di Presidente;
- YYY, nominato dal [AMM2];
- ZZZ, nominato dal [AMM3];
- ....

4. Il Presidente del Comitato Tecnico

Il rappresentante dell'[AMM1] nel CT assume le funzioni di Presidente e di Responsabile di Progetto.
Il Presidente e il Comitato Tecnico possono avvalersi nello svolgimento delle loro funzioni di specialisti tecnici ed amministrativi appartenenti alle Amministrazioni partecipanti ovvero a privati.

5. Modalità di funzionamento e funzioni del CT

Il CT si riunisce almeno su base quindicinale per tutta la durata del Progetto. Di ogni riunione si redige il relativo verbale. Le deliberazioni del CT sono assunte all'unanimità.
Il CT svolge le seguenti funzioni:

- predisposizione degli atti giuridici e tecnici necessari per il Progetto, da sottoporre al CdC per approvazione e il conseguente avviamento del Progetto;
- verifica dell'andamento dei lavori, sulla base delle risultanze delle attività di collaudo/verifica aventi a oggetto i servizi destinati a ciascuna delle Amministrazioni aderenti.

Quest'ultima attività comprende:

- verifica delle attività, più precisamente:
  - verifica dell'effettiva disponibilità di tutti i prodotti e della erogazione dei servizi previsti negli allegati tecnici di cui al Progetto ed ai contratti di fornitura;
  - verifica dello stato di avanzamento dei lavori e analisi degli scostamenti tra pianificato e consuntivato relativamente a obiettivi, tempi, costi e utilizzazione di risorse;
  - valutazione delle eventuali non conformità della fornitura alle specifiche previste, al fine di apprezzare eventuali impatti sull'insieme dell'iniziativa e/o verso l'attuazione di quanto previsto dal Progetto;
  - valutazione degli interventi suggeriti dall'Impresa per sanare le eventuali non conformità impattanti sul Progetto;
  - verifica della attuazione degli interventi di cui all'alinea precedente e verifica degli esiti;

- presa visione e valutazione delle eventuali varianti in corso d'opera, più precisamente:
  - verifica delle cause che hanno prodotto la necessità di varianti al Progetto;
  - analisi della valutazione tecnica ed economica delle varianti;
  - presa visione dei documenti contrattuali a seguito dell'accettazione delle varianti da parte delle Amministrazioni partecipanti;
- monitoraggio degli adempimenti e dei livelli di qualità contrattualmente previsti, più precisamente:
  - verifica del rispetto dei valori di soglia dei livelli di servizio, mediante analisi dei report contrattualmente previsti;
  - analisi delle misurazioni effettuate per seguire l'evoluzione dei fenomeni;
  - valutazione della soddisfazione degli utenti finali interni alle Amministrazioni partecipanti.

Il CT svolge inoltre:

- verifica della compatibilità tra loro dei piani di continuità ed emergenza predisposti dalle singole Amministrazioni partecipanti con riferimento alla concomitanza di più eventi disastrosi;
- analisi dei risultati ottenuti.

Art. 6
Impegni delle Amministrazioni contraenti

1. Approvvigionamenti

L'acquisizione delle tecnologie necessarie per la realizzazione del Progetto sarà curata, nel rispetto dell'autonomia organizzativa di ciascuna Amministrazione, secondo le modalità amministrative ritenute più opportune e con l'osservanza delle norme della Contabilità Generale dello Stato e delle eventuali norme che fossero stabilite per usufruire di particolari forme di finanziamento, in ottemperanza ai vincoli tecnici.
Le caratteristiche tecniche delle apparecchiature HW e SW saranno approvate dal CT per assicurare la rispondenza delle stesse ai requisiti tecnici del Progetto.
Ciascuna delle Amministrazioni coinvolte nel progetto garantirà la disponibilità delle risorse necessarie secondo quanto di seguito riportato:

- AMM1;
- AMM2;
- AMM3;
- .....

Le Amministrazioni firmatarie concordano sin da ora di affidare all'AMM1, e AMM1 accetta, il riferimento per ogni atto relativo all'acquisizione dei servizi di cui al precedente art. 2 (pubblicazione del bando di gara, organizzazione anche logistica della gestione delle

domande e offerte, ecc.), fermo restando che ogni Amministrazione firmataria procederà alla stipula dei singoli contratti di cui all'art. 2.

2. Garanzie

Le Amministrazioni aderenti provvederanno ad attivare clausole contrattuali, nei rapporti con l'Impresa, al fine di prevedere le opportune garanzie in ordine alla puntuale ed esatta realizzazione del Progetto da parte dell'Impresa, ivi compresa, tra l'altro, la clausola secondo la quale il saldo finale dei pagamenti pari ad almeno il XX% sia erogato solo dopo la conclusione positiva del collaudo finale interamministrazioni del sistema.

3. Pianificazione temporale delle attività

L'esito positivo del Progetto è vincolato al rispetto dei tempi definiti dal piano generale previsto nel capitolato tecnico.
Si riportano di seguito le attività che rivestono le maggiori criticità potenziali, dal momento che la loro conclusione condiziona maggiormente il piano del progetto (n.d.r.: DEFINIRE A SECONDA DEL CASO CONCRETO):

- ....
- .....
- ....

Art. 7
Validità del Protocollo di intesa

Il Protocollo d'Intesa sarà approvato dalle Amministrazioni partecipanti al Progetto con Decreto Dirigenziale e avrà efficacia a partire dal giorno successivo a quello in cui il Protocollo risulterà sottoscritto da tutte le Amministrazioni partecipanti.

Appendice D: Modello di contratto

Contratto per la fornitura dei servizi relativi alla continuità operativa

L'anno .... , il giorno .... del mese di .... in .... , via ....

tra

l'Amministrazione, con sede in ...., ..., n. ...., codice fiscale XXXXXXX, di seguito denominata per brevità anche "AMM", in persona di …..........

e

la Società YY ……………………………………….........................., con sede in ...., Via ….............................……………..............., codice fiscale ……...........................…, partita IVA …................................ di seguito denominata per brevità anche "Fornitore", in persona del suo ……………........…………….....

Premesso CHE

- in data... l'AMM, congiuntamente alle amministrazioni AMM2, AMM3, ... ha firmato un protocollo di intesa (nel seguito: Protocollo) avente per oggetto il progetto (nel seguito Progetto) "Acquisizione e gestione di un centro di continuità operativa comune";
- i principali obiettivi del progetto, così come indicati anche nel Protocollo, sono:
  - dotare l'AMM di soluzioni di continuità e/o ripristino per i servizi ICT più critici;
  - realizzare economie di scala e organizzative condividendo servizi e risorse;
  - standardizzare le metodologie nel campo della disponibilità dei sistemi ICT;
  - diffondere il know-how e la sensibilità sui temi della continuità operativa, dei livelli di servizio e gestione dell'emergenza;
- le attività di predisposizione delle strutture di gestione previste nel Protocollo si sono concluse con la costituzione del Comitato di Coordinamento (CdC) e del Comitato Tecnico (CT) previsti all'articolo 5 dello stesso Protocollo;
- il CT, come previsto all'articolo 5 del Protocollo, ha predisposto in data....la proposta tecnico-economica (di seguito Proposta) per la realizzazione del Progetto da sottoporre all'approvazione del CdC;
- il CdC ha approvato la Proposta in data..., dando così avvio alla realizzazione del Progetto;
- ai sensi dell'art. 5 del Protocollo, il CT sovrintende alla realizzazione del Progetto;

- lo schema del presente atto, unitamente alla restante documentazione di gara, è stato sottoposto, ai sensi dell'art. 8 del decreto legislativo 12 febbraio 1993, n. 39, al parere di congruità tecnico-economica del CNIPA che si è espresso con esito favorevole in data ……………… con parere n. ……………;
- come previsto dalla Proposta, con bando pubblicato nella Gazzetta Ufficiale della Repubblica Italiana il .... e nella Gazzetta Ufficiale della Comunità Europea il ...., è stata indetta una gara per ....
- detta gara è stata aggiudicata al Fornitore;

OPPURE IN CASO DI TRATTATIVA PRIVATA ELIMINARE I RIFERIMENTI ALLA PROCEDURA DI GARA E MOTIVARE TALE TIPOLOGIA DI AGGIUDICAZIONE

VISTI

(NOTA: eliminare i riferimenti non applicabili alla singola amministrazione)

- la Direttiva del Ministro per l'innovazione e le tecnologie del 16 gennaio 2002 in materia di "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali" (Gazz. Uff. n. 69 del 22 marzo 2002);
- l'art. 1, commi 192, 193 e 194 della legge 30 dicembre 2004 n. 311 (Finanziaria 2005);
- l'art. 3, lettera c) del DPCM 31 maggio 2005 (Gazz. Uff. 18 giugno 2005, n. 140) recante "Razionalizzazione in merito all'uso delle applicazioni informatiche e servizi ex articolo 1, commi 192, 193 e 194 della legge n. 311 del 2004 (Finanziaria 2005)";
- il Decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale;
- il DPCM 6 agosto 1997, n. 452 (Gazz. Uff. 30 dicembre 1997, n. 302);
- *… altri riferimenti di legge propri dell'amministrazione medesima;*

tutto ciò premesso e considerate le premesse parte integrante e sostanziale del presente atto,

si conviene e si stipula quanto segue

Art. 1

Oggetto del Contratto – Modalità di erogazione dei Servizi – Allegati

Il presente Contratto con i suoi allegati definisce modalità, condizioni e termini generali in base ai quali il Fornitore assume l'obbligo di fornire all'AMM l'insieme degli specifici servizi (di seguito "Servizi") necessari per garantire all'AMM la continuità operativa.
I Servizi sono definiti nella loro configurazione nell'allegato n. 1 "…." (Offerta Tecnica oppure Capitolato Tecnico) al presente Contratto, del quale è parte integrante e sostanziale.
I Servizi sono i seguenti: (*nota interna:* l'AMM dovrà qui inserire le classi di servizio che costituiranno l'oggetto del contratto; a tal fine, si riporta a titolo di esempio l'elencazione di tutte le classi di servizio potenzialmente oggetto di contratto):

a) servizi di progettazione/realizzazione della soluzione di Continuità Operativa e di adeguamento del progetto e del piano di continuità operativa alle modifiche evolutive del sistema dell'AMM;

b) servizi di manutenzione delle componenti hardware di cui alla lettera i) del successivo art. 3[71];

c) servizi di conduzione sistemistica e operativa post-realizzazione della soluzione di Continuità Operativa dell'AMM, nonché delle eventuali ulteriori componenti software di cui alla lettera i) del successivo art. 3[72];

d) messa a disposizione, esclusivamente nei locali qui sotto indicati (nel seguito per brevità "Locali")[73]:
   - locali di via... in...
   - locali di via... in...

   dove sono ubicati i locali dedicati all'erogazione da parte del Fornitore del servizio di Continuità Operativa, di spazi informatici attrezzati e gestiti e dai relativi servizi di logistica e sorveglianza;

e) servizi di risorse elaborative[74].

---

[71] Comprendenti, a titolo esemplificativo e non esaustivo, attività relative all'affidamento al fornitore del servizio di manutenzione hardware delle apparecchiature rientranti nella disponibilità dell'AMM e costituenti parte o tutta la configurazione della soluzione di Continuità Operativa.

[72] Comprendenti, a titolo esemplificativo e non esaustivo, attività come:

- esercizio operativo delle apparecchiature e delle componenti software previste nella soluzione di Continuità Operativa, in termini di controllo e monitoraggio del funzionamento, eventuale ripristino dopo interruzioni, eventuale salvataggio e archiviazione di log, back-up, ecc., tracciatura e gestione dei problemi riscontrati, pianificazione e coordinamento degli interventi di manutenzione ordinaria e straordinaria;
- aggiornamento del livello del software di base e di ambiente, sulla base delle specifiche fornite dall'AMM;
- predisposizione dell'ambiente per lo svolgimento dei test periodici o per gestire lo switch in casi di dichiarazione di disastro;
- allineamento delle configurazioni alle evoluzioni del progetto di Continuità Operativa, secondo le specifiche dell'AMM.

[73] Comprendenti, a titolo esemplificativo e non esaustivo, attività come:

- messa a disposizione da parte del fornitore di locali attrezzati a CED per la installazione e messa in funzione delle apparecchiature costituenti la soluzione di Continuità Operativa; lo spazio dovrà essere opportunamente attrezzato in termini di alimentazione elettrica sempre e comunque disponibile, garantita attraverso gruppi di continuità e auto generatori, condizionamento ambientale della temperatura, protezione dagli accessi fisici non autorizzati, protezione antincendio e antiallagamento;
- messa a disposizione da parte del fornitore di locali da adibire ad uffici per ospitare personale dell'AMM nel corso dei test operativi ed in caso di dichiarazione di disastro; i locali dovranno essere attrezzati con tavoli da lavoro forniti di prese elettriche, attacchi alla rete LAN, collegamento telefonico;
- messa a disposizione di locali e/o armadi opportunamente protetti per la conservazione di supporti magnetici o ottici e di documenti, secondo quanto previsto dal piano di contingency;
- ritiro, trasporto e consegna di materiali dell'AMM, quali supporti magnetici e/o ottici, documenti, carta per stampanti.

[74] Comprendenti, a titolo esemplificativo e non esaustivo, attività come:

- messa a disposizione da parte del fornitore di risorse elaborative, quali server o partizioni logiche o fisiche di server di qualunque classe, storage, librerie robotizzate per supporti magnetici o ottici, apparati di rete locale o geografica, firewall o altri apparati costituenti la configurazione del sistema di back-up;
- messa a disposizione di licenze software, eventualmente necessarie alla operatività della soluzione;
- messa a disposizione di Personal Computer, stampanti, scanner necessari sia per la gestione ed il controllo dei sistemi, sia per completare l'attrezzaggio dei posti di lavoro messi a disposizione del personale dell'AMM.

I Servizi saranno erogati nel rispetto delle modalità, condizioni e termini di cui al presente Contratto e suoi allegati.
L'AMM potrà richiedere al Fornitore l'erogazione dei Servizi nei casi di Disastro (di seguito "Caso di Disastro") descritti nell'Allegato 1.
La modalità di fruizione dei Servizi è la seguente:
(NOTA INTERNA: si riportano le due soluzioni a scelta dell'AMM; ovviamente dette soluzioni avranno costi diversi)

1ª SOLUZIONE – Modalità illimitata

In "Caso di Disastro" i Servizi di cui al paragrafo XX dell'Allegato 1 (NOTA INTERNA: sono i servizi erogati per assicurare l'operatività dopo l'avvenuto disastro) saranno erogati dal Fornitore a far tempo dalla data della dichiarazione di "Caso di Disastro" e fino alla avvenuta ricostituzione dell'infrastruttura dell'AMM colpita dall'evento disastroso e comunque nel rispetto del termine di durata del presente contratto.

2ª SOLUZIONE – Modalità limitata

a) In "Caso di Disastro" i Servizi di cui al paragrafo XX dell'Allegato 1 (NOTA INTERNA: sono i servizi erogati per assicurare l'operatività dopo l'avvenuto disastro) saranno erogati dal Fornitore a far tempo dalla data della dichiarazione di "Caso di Disastro" e per un periodo massimo di XXX giornate lavorative a fronte del corrispettivo di cui all'Allegato 2 punto XX;
b) Allo scadere del periodo di cui alla precedente lettera a), l'AMM potrà richiedere al Fornitore, che sin da ora si obbliga conseguentemente, di usufruire della stessa infrastruttura e degli stessi livelli di Servizio a fronte del corrispettivo di cui all'Allegato 2 punto ZZ.

Al presente Contratto si allegano:

- sub n. 1 "...." (Offerta Tecnica o Capitolato Tecnico);
- sub n. 2 "Offerta Economica";
- …

ART. 2
Durata ed efficacia

Il presente contratto ha durata dalla data del suo perfezionamento fino al gg/mm/aaaa.
Il presente Contratto, mentre è vincolante per il Fornitore dalla data di sottoscrizione, esplicherà la sua efficacia, per l'AMM, solo dopo la sua approvazione nelle forme di legge. Di tale approvazione l'AMM darà tempestiva comunicazione al Fornitore mediante lettera raccomandata con avviso di ricevuta, anticipata via fax.

ART. 3
Impegni specifici del Fornitore

Il Fornitore si obbliga a:

a) adempiere esattamente tutte le obbligazioni dal Fornitore medesimo assunte con la sottoscrizione del presente Contratto e dei suoi allegati;

b) gestire a proprio carico i locali della struttura presso cui vengono erogati i servizi di Continuità Operativa di cui al presente Contratto e suoi allegati;

c) erogare i servizi di cui al presente Contratto e suoi allegati secondo le modalità, i termini, le condizioni contrattuali ed economiche e le specifiche indicate nel presente Contratto e nei suoi allegati;

d) assicurare i livelli di servizio previsti al successivo art. 7;

e) rendere disponibili all'AMM i risultati delle misure effettuate sui citati livelli di servizio con le modalità ed i tempi di cui al successivo art. 7;

f) fornire i servizi di cui al presente Contratto e nei relativi allegati impiegando, a propria cura e spese, tutte le infrastrutture, anche informatiche, ed il personale necessario per la erogazione degli stessi secondo quanto specificato dal presente Contratto e dai suoi allegati;

g) osservare nei confronti dei propri dipendenti, occupati nelle attività oggetto del presente Contratto, le condizioni normative e retributive stabilite dai contratti collettivi di lavoro relativi alla categoria, nonché le condizioni risultanti da successive modifiche ed integrazioni ed in genere da ogni altro contratto collettivo successivamente stipulato per la categoria, applicabile nella località di esecuzione del contratto; il Fornitore si obbliga, altresì, a continuare ad applicare i suindicati contratti collettivi anche dopo la loro scadenza e fino alla loro sostituzione. I suddetti obblighi vincolano il Fornitore anche nel caso in cui lo stesso non aderisca alle associazioni stipulanti o receda da esse. Nel caso di violazione degli obblighi di cui sopra e previa comunicazione al Fornitore delle inadempienze denunciate dalla amministrazione competente, l'AMM si riserva il diritto di operare una ritenuta pari, al massimo, al 20% (ventipercento) dell'importo dovuto al Fornitore ai sensi del presente Contratto. Tale ritenuta sarà rimborsata soltanto quando la competente amministrazione avrà dichiarato che il Fornitore si è posto in regola; il Fornitore non potrà vantare diritto alcuno per il ritardato pagamento. Con il presente Contratto non viene instaurato alcun rapporto di lavoro tra l'AMM e le persone di cui il Fornitore si avvarrà per l'esecuzione delle attività di cui al presente Contratto. La remunerazione di tali persone fa carico integralmente ed esclusivamente al Fornitore;

h) (DISCREZIONALE) rispettare, per quanto applicabili, le seguenti norme internazionali: ... .

i) consentire all'AMM l'installazione presso i locali del Centro di CO di componenti hardware e software, descritte nell'Allegato 1, rientranti nella disponibilità dell'AMM, necessarie all'AMM medesima per il conseguimento degli obiettivi di Continuità Operativa. In relazione alle citate componenti rientranti nella propria disponibilità, l'AMM s'impegna a garantire livelli di servizio tali da non pregiudicare l'esatta esecuzione delle obbligazioni assunte dal Fornitore con la sottoscrizione del presente

Contratto. L'installazione di tali componenti avverrà in conformità alle modalità, condizioni e termini previsti nell'Allegato 1 e con un preavviso di almeno 20 (venti) giorni solari prima di quello in cui dovrà avvenire l'installazione. Resta inteso che il Fornitore sarà responsabile soltanto delle obbligazioni dallo stesso assunte con la firma del presente Contratto. Le attività di trasporto, installazione, disinstallazione di tali componenti restano a carico de ...;

j) consentire al personale dell'AMM l'accesso ai Locali, al fine di verificare l'esatto adempimento da parte del Fornitore di tutte le obbligazioni assunte dal medesimo con la sottoscrizione del presente Contratto.

Art. 4
Documentazione da produrre

Il Fornitore si impegna a predisporre e consegnare all'AMM, entro 40 (quaranta) giorni solari dalla firma del presente Contratto, la seguente documentazione:

a) piano della qualità di dettaglio;
b) piano di progetto di dettaglio dei servizi di cui al presente Contratto e suoi allegati;
c) descrizione delle misure di protezione fisica attive e passive presenti presso i Locali;
d) specifiche del servizio, specifiche di realizzazione del servizio e specifiche di controllo qualità del servizio;
e) piano di Collaudo di cui al successivo art. 9.

Il Fornitore consegnerà inoltre all'AMM il Manuale Tecnico, Organizzativo e Utente del Piano di Ripristino che prevedrà:

a) Modalità di attivazione del servizio;
b) Accordi di servizio interni ed accordi di servizio con fornitori esterni;
c) Descrizione della rete di back up;
d) Descrizione delle procedure di ripristino e ripartenza dei servizi informatici (sistemi, dati e rete);
e) Descrizione delle procedure di restart dei servizi forniti da provider esterni (servizi istituzionali);
f) Inventari delle applicazioni, delle apparecchiature e dei documenti vitali;
g) Processo di attuazione del piano;
h) Descrizione dei criteri di esecuzione delle prove;
i) Log degli aggiornamenti al documento;
j) Procedura di rientro al CED primario.

Art. 5
Ruolo del Comitato di Coordinamento e del Comitato Tecnico

Con riferimento a quanto contenuto nel Protocollo, il Fornitore prende atto che al Comitato di Coordinamento (di seguito CdC) ed al Comitato Tecnico (di seguito CT) di

cui all'art. 5 del "Protocollo" sono attribuite le funzioni ivi rispettivamente descritte che il Fornitore dichiara di avere letto, di ben conoscere e di accettare; le citate funzioni del CT rilevanti ai fini del presente Contratto sono, in particolare:

- verifica dell'andamento dei lavori, sulla base delle risultanze delle attività di collaudo/verifica delle singole Amministrazioni, che comprende:
  - verifica delle attività:
    - verifica dell'effettiva disponibilità di tutti i prodotti e della erogazione dei servizi previsti negli allegati tecnici ai contratti di fornitura;
    - verifica dello stato di avanzamento dei lavori e analisi degli scostamenti tra pianificato e consuntivato relativamente a obiettivi, tempi, costi e utilizzazione di risorse;
    - valutazione delle eventuali non conformità della fornitura alle specifiche previste nel singolo Contratto di fornitura al fine di apprezzare eventuali impatti sull'insieme dell'iniziativa e/o verso l'attuazione di quanto previsto in altri singoli contratti;
    - analisi delle cause della non conformità, anche attraverso l'esame delle registrazioni di qualità che documentano la loro esecuzione;
    - approvazione degli interventi ritenuti opportuni dal Fornitore per sanare la non conformità che ha impatti sul Progetto;
    - controllo della attuazione degli interventi di cui all'alinea precedente e verifica degli esiti;
  - presa visione e valutazione delle eventuali varianti in corso d'opera:
    - verifica delle cause, endogene ed esogene al contratto, che hanno prodotto la necessità di varianti;
    - analisi della valutazione tecnica ed economica delle varianti;
    - presa visione dei documenti contrattuali a seguito dell'accettazione delle varianti da parte delle amministrazioni;
  - monitoraggio degli adempimenti e dei livelli di qualità contrattualmente previsti:
    - verifica del rispetto dei valori di soglia dei livelli di servizio, mediante analisi dei report contrattualmente previsti;
    - analisi delle misurazioni effettuate, per seguire l'evoluzione dei fenomeni;
    - valutazione della soddisfazione degli utenti finali interni alle amministrazioni;
- verifica della compatibilità tra loro dei piani di continuità ed emergenza predisposti dalle singole Amministrazioni partecipanti con riferimento alla concomitanza di più eventi disastrosi;
- analisi dei risultati ottenuti.

ART. 6
Fasi del Progetto – Modalità di erogazione dei servizi

La realizzazione del Progetto si suddivide in due fasi progettuali:

- Fase di Setup
- Fase di Esercizio.

La fase di Setup prevede l'erogazione di attività da parte del Fornitore sia presso il Sito Primario dell'AMM, sia presso i Locali, al fine di disegnare e realizzare la soluzione descritta nell'Allegato 1.
Al termine della Fase di Setup la soluzione sarà fruibile dall'AMM ed avrà inizio la Fase di Esercizio che avrà durata pari alla durata del presente Contratto.
La Fase di Setup avrà una durata massima di xxx mesi a partire dalla data di sottoscrizione del presente Contratto.
La Fase di Esercizio inizierà dopo il collaudo positivo della Fase di Setup.
La Fase di Setup del Progetto si concluderà a fronte del superamento del collaudo con esito positivo della soluzione realizzata.

ART. 7
Livelli di servizio e penali

Il Fornitore si obbliga a rispettare i livelli di servizio indicati nella tabella che segue. In caso di inadempimento di tale obbligazione, al Fornitore saranno applicate le penalità indicate nella tabella medesima, fatto salvo il risarcimento di ogni eventuale ulteriore danno derivante dal mancato rispetto delle obbligazioni tutte assunte dal Fornitore con la sottoscrizione del presente Contratto.
I valori economici da utilizzare quale base di calcolo delle penalità sono riportati nella Offerta economica del Fornitore.
Le penali applicabili non potranno superare cumulativamente il 10% dell'importo contrattuale.

PERIODO	SERVIZIO	ATTIVITÀ	LIVELLI DI SERVIZIO	UNITÀ DI MISURA	MODALITÀ DI VERIFICA	BASE DI CALCOLO DELLA PENALE	PENALE APPLICABILE E NEL PERIODO CONTRATTUALE
Setup	Progettazione/ realizzazione e manutenzione del piano della soluzione	Progettazione/ realizzazione della soluzione	Pronti al collaudo entro 180 giorni dalla data di efficacia contrattuale	Numero di giorni di ritardo nel completamento dell'attività	Verbale di collaudo positivo	Importo dell'attività	Per ogni giorno di ritardo lo 0,5% dell'importo della base di calcolo fino ad un massimo di 20 gg di ritardo
Setup	Messa a disposizione degli spazi informatici (Housing)	Allestimento degli spazi informatici	Disponibilità degli spazi nella q.tà prevista in Allegato sub. 1 entro 45 gg. dalla data di efficacia contrattuale	Numero di giorni di ritardo nella consegna degli spazi	Verbale di consegna degli spazi	Importo dell'attività di allestimento degli spazi	0,5% della base di calcolo per ogni giorno di ritardo sulla data di consegna prevista fino ad un massimo di 20 giorni di ritardo
Setup	Risorse elaborative	Predisposizione risorse elaborative	Impostazione dei prodotti previsti come Configurazione di emergenza nell'Allegato sub. 1 e superamento dei test funzionali entro 60 giorni dalla data di efficacia contrattuale	Numero di ore di indisponibilità degli spazi dopo l'allestimento	Verbale di installazione (collaudo positivo)	15% dell'importo del Servizio Risorse elaborative	Per ogni giorno di ritardo lo 0,5% dell'importo dell'attività fino ad un massimo di 20 giorni di ritardo

(segue)

Setup/ Esercizio	Messa a disposizione degli spazi informatici (Housing)	Disponibilità degli spazi attrezzati (e gestiti)	Garantire la corretta continuità operativa degli impianti tecnologici	Numero di ore di indisponibilità degli spazi dopo l'allestimento	Verbale di verifica mensile	importo pari a 12 mensilità del servizio di housing	0,3% della base di calcolo per ogni ora non pianificata di interruzione del servizio informatco per cause imputabili agli impianti tecnologici (fermi programmati non superiori a tre (3) gg/anno fino ad un massimo di 36 ore
Setup/ Esercizio	Messa a disposizione degli spazi informatici (Housing)	Disponibilità degli spazi attrezzati (e gestiti)	Garantire la corretta continuità operativa degli impianti tecnologici	Numero di ore di indisponibilità degli spazi dopo l'allestimento	Verbale di verifica mensile	Importo pari a 12 mensilità del servizio di housing	0,3% della base di calcolo per ogni ora non pianificata di interruzione del servizio informatco per cause imputabili agli impianti tecnologici (fermi programmati non superiori a tre (3) gg/anno fino ad un massimo di 36 ore
Esercizio	Progettazione/realizzazione della soluzione	Manutezione della soluzione	Esecuzione con esito positivo di 2 test annuali programmati, secondo le modalità descritte nell'Allegato sub. 1	Numero di settimane di ritardo per la risoluzione di problemi in caso di test con esito negativo	Verbale di verifica mensile	Importo annuale del servizio di Assistenza operativa e manutenzione della soluzione	1% della base di calcolo ogni giorno di ritardo per un massimo di 5 giorni
Esercizio	Risorse elaborative	Disponibilità delle risorse elaborative [Attività della Configurazione di emergenza (apparecchiature dedicate)]	Termine dello startup delle apparecchiature dedicate entro 2 ore solari dalla richiesta, anche telefonica fatta dal Responsabile dell'Istituto	Ore di indisponibilità	Verbale di verifica mensile	Importo pari a 12 mensilità dal servizio di Risorse elaborative	1% della base di calcolo ogni ora di ritardo, oltre le 2 (due) previste fino ad un massimo di 8 (otto) ore di ritardo

Definizioni della suindicata Tabella:

PERIODO
Rappresenta uno dei due periodi in cui è suddiviso il presente contratto di servizi.

SERVIZIO
Definisce uno dei cinque servizi in cui è suddiviso il presente contratto.

ATTIVITÀ
Definisce la specifica attività, sottocomponente del servizio relativo, a cui si riferisce l'indicatore/misuratore.

LIVELLI DI SERVIZIO
Definisce gli impegni che l'Impresa assume verso l'Istituto in merito alla qualità del servizio erogato.

UNITÀ DI MISURA
Definisce il singolo valore, al superamento del quale non si considerano rispettati i livelli di servizio attesi, e la prestazione deve essere considerata passibile di applicazione di penalità.

MODALITÀ DI VERIFICA
Definisce la modalità di verifica e di documentazione della misurazione del livello di servizio.

BASE CALCOLO DELLA PENALE
Riporta il criterio per calcolare l'importo della penale.

PENALE APPLICABILE
Si intende la valorizzazione degli importi applicabili per ciascuna inadempienza rilevata.

ART. 8
Prezzi unitari, corrispettivi, modalità di pagamento e revisione prezzi

I corrispettivi dovuti al Fornitore dall'AMM per l'erogazione dei servizi di cui al presente Contratto sono specificati nell'allegato sub n. 2 "Offerta Economica".
Qualora nel corso dell'esecuzione del Contratto si dovessero verificare eventi imprevedibili, comportanti un aumento o una diminuzione del costo dei materiali o della mano d'opera, tali da determinare una variazione superiore al decimo del prezzo complessivo convenuto, il Fornitore o l'AMM possono chiedere una revisione del prezzo, che può essere accordata solamente per quella differenza che eccede il decimo, con cadenza annuale a decorrere dal .... (primo/secondo/terzo o altro) anno da stabilire a cura dell'AMM.
Nel caso di aumento, la revisione avverrà solo a seguito di richiesta scritta inviata tramite racc. A.R. e decorrerà dal primo giorno del mese successivo.
La revisione verrà operata sulla base di una istruttoria condotta dal Dirigente responsabile del progetto, in conformità con quanto disposto dall'art. 115 del D.Lgs. 12 aprile 2006, n. 163.
I pagamenti sono disposti in base alle seguenti modalità:

- su presentazione di fatture posticipate a fronte dei collaudi positivi di attività (pagamenti una tantum);
- su presentazione di fatture (periodo: mensili, trimestrali, ecc.) posticipate, previa attestazione da parte dell'AMM della regolarità dei servizi ricevuti (pagamento di canoni).

Il pagamento di tali fatture, che dovranno essere inviate in originale e in duplice copia all'AMM, avrà luogo entro 60 (sessanta) giorni solari dalla ricezione delle stesse, fermo restando quanto di seguito indicato relativamente alle attestazioni della regolare esecuzione della fornitura e previa detrazione degli eventuali crediti dell'AMM derivanti dal mancato versamento di contributi assicurativi.
Le disposizioni di cui al decreto legislativo n. 231/2002 in merito agli interessi dovuti in caso di ritardato pagamento troveranno applicazione solo previa richiesta scritta, con assegnazione di un termine non inferiore a 15 (quindici) giorni solari, da effettuarsi a mezzo lettera raccomandata a.r. dal Fornitore, per porre fine all'eventuale ritardo.

ART. 9
Collaudo – Verifiche

I servizi di cui all'art. 1 sono sottoposti a collaudo dall'AMM al fine di verificare la conformità di detti servizi con le specifiche di dettaglio di cui al presente Contratto e all'Allegato 1.
A tal fine, entro 40 (quaranta) giorni solari dalla sottoscrizione del presente atto, il Fornitore presenterà per l'accettazione all'AMM il "Piano di Collaudo".
Il Piano di Collaudo conterrà almeno i seguenti elementi:

- oggetto del collaudo;

- natura e volumi dei casi di prova;
- risorse impiegate (sia dal Fornitore che dall'amministrazione collaudante) relativamente a personale, competenze, locali, apparecchiature e documentazione;
- tempificazione delle attività di collaudo;
- specifiche di dettaglio delle prove di collaudo, comprensive della definizione dei casi di prova, dei criteri di superamento, delle date di effettuazione del collaudo.

Il Fornitore e l'AMM potranno concordare eventuali modifiche al Piano di Collaudo entro 15 (quindici) giorni solari a far data dalla presentazione del Piano di Collaudo medesimo.
Le prove di collaudo saranno eseguite dall'AMM, in presenza e con la collaborazione del Fornitore, nei modi specificati e concordati nel Piano di Collaudo entro i termini indicati nel Piano stesso.
Il collaudo sarà considerato positivamente superato qualora tutti i risultati siano conformi ai criteri di superamento, specificati nel Piano di Collaudo. Al termine del collaudo con esito positivo, verrà redatto apposito verbale sottoscritto anche dal Fornitore, al quale ne verrà consegnata copia.
In caso di esito negativo del collaudo, il Fornitore dovrà provvedere a correggere le anomalie riscontrate e ad effettuare nuovamente il Collaudo entro 20 (venti) giorni solari dalla data del verbale di collaudo negativo.
Nel caso in cui anche il secondo collaudo risultasse negativo, l'AMM, valutata la natura e l'entità delle anomalie riscontrate, potrà, a propria discrezione:

- concedere, fermo restando l'applicazione delle relative penali previste al precedente art. 7 e fatto salvo il risarcimento di ogni eventuale ulteriore danno, un ultimo termine non superiore a 10 (dieci) giorni solari, per la rimozione definitiva dei vizi e difetti riscontrati nel secondo collaudo;
- risolvere il presente Contratto, fatto salvo il diritto al risarcimento di tutti i danni diretti ed indiretti comunque subiti dall'AMM.

Art. 10
Varianti tecnologiche

In qualunque momento, l'AMM o il Fornitore potranno chiedere, mediante richiesta scritta all'altra parte, modifiche all'allegato sub 1 al presente Contratto.
In caso di richiesta di modifica presentata dal Fornitore, l'AMM, notificherà al Fornitore il proprio parere in merito all'attuazione della modifica proposta entro 30 (trenta) giorni solari dal ricevimento della relativa richiesta. Per quanto previsto all'articolo 5 del presente Contratto, l'AMM si riserva di verificare preliminarmente, dopo comunicazione al CdC, i contenuti delle varianti anche al fine di garantire la coerenza delle varianti stesse alle finalità del Progetto.
Qualora sia l'AMM a chiedere la variazione, il Fornitore, entro 30 (trenta) giorni solari dal ricevimento della richiesta medesima, notificherà all'AMM se tale variazione potrà essere effettuata e quali effetti essa produrrà ai termini, anche economici, e alle condizioni di cui al presente Contratto.

ART. 11
Controversie

Qualora non fosse possibile raggiungere un accordo su eventuali controversie riguardanti l'interpretazione o l'esecuzione del presente Contratto e, comunque, una volta decorsi inutilmente 60 (sessanta) giorni solari dall'insorgere delle stesse, ciascuna delle parti potrà deferire la questione ad un Collegio arbitrale nel rispetto di quanto stabilito dall'art. 241 del D.Lgs. 12 aprile 2006, n. 163.

ART. 12
Riservatezza

Il Fornitore si impegna a non portare a conoscenza di terzi informazioni, dati, documenti e notizie di carattere riservato, di cui il personale comunque impiegato nello svolgimento delle attività oggetto del presente Contratto venga a conoscenza in forza del presente contratto.
L'obbligo di riservatezza continuerà a permanere in capo al Fornitore per il periodo di un anno oltre il termine di durata del presente Contratto.

ART. 13
Recesso e risoluzione

Ai sensi dell'art. 1373 del codice civile, l'AMM avrà la facoltà di recedere dal presente Contratto tramite raccomandata A.R. da inviare al Fornitore con un preavviso di almeno dodici mesi.
Il Fornitore rinuncia sin da ora a qualsiasi eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore indennizzo e/o rimborso, anche in deroga a quanto previsto dall'articolo 1671 cod. civ. Sono fatte salve le prestazioni già rese.
Nel caso di mancata o inesatta esecuzione da parte del Fornitore anche di uno solo degli obblighi assunti dal Fornitore medesimo con la sottoscrizione del presente Contratto, l'AMM potrà, ai sensi dell'art. 1454 cod. civ., risolvere il Contratto previa diffida ad adempiere nel termine di 30 (trenta) giorni solari dal ricevimento della diffida medesima, da trasmettersi al Fornitore anche via fax o con raccomandata A.R.
Se entro il citato termine il Fornitore non avrà posto rimedio all'inadempimento totale o parziale, il Contratto si intenderà risolto, fatto salvo il diritto al risarcimento di ogni danno.
In ogni caso, il presente Contratto si risolverà di diritto per i seguenti motivi:

- nel caso in cui sia stato depositato contro il Fornitore un ricorso ai sensi della legge fallimentare o di altra legge applicabile in materia di procedure concorsuali, che proponga lo scioglimento, la liquidazione, la composizione amichevole, la ristrutturazione dell'indebitamento o il concordato con i creditori, ovvero nel caso in cui venga designato un liquidatore, curatore, custode o soggetto avente simili funzioni, il quale entri in possesso dei beni o venga incaricato della gestione degli affari del Fornitore;
- nel caso in cui taluno dei componenti l'organo di amministrazione o l'amministratore delegato o il direttore generale o il responsabile tecnico del Fornitore siano

condannati, con sentenza passata in giudicato, per delitti contro la Pubblica Amministrazione, l'ordine pubblico, la fede pubblica o il patrimonio, ovvero siano assoggettati alle misure previste dalla normativa antimafia.

Art. 14
Responsabilità civile

Il Fornitore assume in proprio ogni responsabilità per infortunio o danni, diretti ed indiretti, eventualmente subiti da persone o da beni, tanto del Fornitore quanto dell'AMM o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso Fornitore riferibili, anche se eseguite da parte di terzi.

Art. 15
Deposito cauzionale

A garanzia dell'esatto adempimento delle obbligazioni assunte con la sottoscrizione del presente Contratto, il Fornitore è tenuto a versare all'AMM, entro 10 giorni dalla sottoscrizione del presente Contratto, un deposito cauzionale pari al 10% del corrispettivo del presente Contratto con le modalità previste dalla documentazione di gara (in caso di procedura concorrenziale).

oppure

con le seguenti modalità (in caso di trattativa privata)
.....
.....
.....

Art. 16
Brevetti e Diritti d'autore

L'AMM non assume alcuna responsabilità ove il Fornitore abbia usato, per le prestazioni oggetto del presente Contratto, dispositivi o soluzioni tecniche di cui altri abbiano ottenuto la privativa.
Il Fornitore manleva e tiene indenne l'AMM da tutte le rivendicazioni legali, le responsabilità, le perdite ed i danni pretesi da qualsiasi persona, a seguito di qualsiasi rivendicazione di violazione di diritti d'autore, di marchio e/o di brevetti italiani o stranieri.
L'AMM informerà prontamente per iscritto il Fornitore delle rivendicazioni di cui al precedente comma. Il Fornitore si obbliga a prestare ogni collaborazione alla AMM al fine della positiva risoluzione della questione.
L'AMM riconosce al Fornitore la facoltà:

- di far ottenere all'AMM ed a spese del Fornitore medesimo il diritto di continuare ad usare i dispositivi o le soluzioni tecniche in questione di cui altri abbiano otte-

nuto la privativa, fatto sempre salvo l'obbligo del risarcimento del danno a carico del Fornitore; oppure

- di sostituire o modificare, a cura e spese del Fornitore, tali dispositivi o soluzioni tecniche in modo che non violino più brevetti o diritti d'autore, fatto sempre salvo l'obbligo del risarcimento del danno a carico del Fornitore; oppure
- di ritirare, a cura e spese del Fornitore, detti dispositivi o soluzioni tecniche se nessuna delle precedenti alternative fosse ragionevolmente attuabile, fatto sempre salvo l'obbligo sia del risarcimento del danno a carico del Fornitore sia della esatta esecuzione delle obbligazioni assunte dal Fornitore medesimo con la sottoscrizione del presente Contratto.

Art. 17
Proprietà

Resta espressamente convenuto che non avverrà alcun trasferimento dei diritti di proprietà o di sfruttamento economico dei programmi su licenza forniti nel presente Contratto.

Art. 18
Responsabile di progetto

Per consentire una corretta esecuzione delle prestazioni oggetto del presente Contratto, sarà cura del Fornitore e dell'AMM, provvedere a comunicarsi per iscritto, entro 15 (quindici) giorni solari dalla data di stipula del presente Contratto, i nominativi dei rispettivi responsabili del progetto che rappresenteranno il Fornitore e l'AMM nei reciproci rapporti e che avranno la responsabilità di concordare i modi e i tempi di attuazione del Piano di Progetto.

Art. 19
Impegni dell'AMM

Sarà cura dell'AMM provvedere a quanto segue:

- assicurare la partecipazione delle proprie figure professionali e tecniche alle sessioni di pianificazione ed alle sessioni di lavoro necessarie allo svolgimento delle attività previste;
- fornire tutte le informazioni che saranno richieste, tramite interviste, verifiche o ricognizioni, se necessarie alla predisposizione ed esecuzione di quanto oggetto del presente Contratto;
- fornire eventuale supporto sistemistico e applicativo necessario al corretto sviluppo del progetto;
- in caso di dichiarazione di disastro, integrare con personale operativo dell'AMM gli operatori del Fornitore; il personale opererà sotto l'esclusiva responsabilità dell'AMM, presso il sito predisposto dal Fornitore, per la tutta la durata del disastro, al

fine di garantire il servizio informatico all'utenza dell'AMM; in caso di disastro dovrà essere presente un rappresentante dell'AMM, presso il sito del Fornitore, responsabile di assumere le decisioni operative di pertinenza dell'AMM;

- verificare ed approvare i risultati delle analisi ed i piani di realizzazione;
- consentire ai tecnici del Fornitore l'utilizzo dei prodotti di proprietà dell'AMM necessari allo svolgimento delle attività;
- consentire, per gli scopi collegati alle funzioni di Continuità Operativa, l'accesso ai locali del proprio CED al personale tecnico del Fornitore.

Art. 20
Oneri fiscali e Spese contrattuali

Il Fornitore riconosce a proprio carico tutti gli oneri fiscali e tutte le spese contrattuali relative al presente atto.
Al presente atto dovrà essere applicata l'imposta di registro in misura fissa, ai sensi dell'art. 40 del DPR 26 aprile 1986, n. 131 e successive modificazioni e integrazioni.

Art. 21
Domicilio legale

Per i fini e gli effetti di cui al presente Contratto, il Fornitore elegge il proprio domicilio legale in ………, Via ………

Art. 22
Manleva

Il Fornitore assume ogni obbligazione nei confronti dei contraenti e terzi aventi rapporti con esso medesimo e terrà sollevata ed indenne l'AMM da ogni controversia e da eventuali oneri che possano derivare da contestazioni, riserve, pretese, azioni risarcitorie di imprese affidatarie, fornitori e terzi, direttamente o indirettamente relative o connesse all'esecuzione del presente.

Art. 23
Trattamento dei dati – Consenso al trattamento

Ai sensi di quanto previsto dal decreto legislativo n. 196 del 2003, ogni parte dichiara di essere stata preventivamente informata dall'altra, prima della sottoscrizione del presente Contratto, circa le modalità e le finalità del trattamento dei propri dati personali che verrà effettuato dall'altra parte per l'esecuzione del presente Contratto. Ogni parte dichiara

espressamente di acconsentire al trattamento da parte dell'altra dei propri dati per le finalità connesse all'esecuzione del presente Contratto.
A tal fine, le parti dichiarano che i dati personali forniti con il presente atto sono esatti e corrispondono al vero, esonerandosi reciprocamente da qualsivoglia responsabilità per errori materiali di compilazione, ovvero per errori derivanti da una inesatta imputazione dei dati stessi negli archivi elettronici e cartacei.
Il trattamento dei dati sarà improntato ai principi di correttezza, liceità e trasparenza e nel rispetto delle misure di sicurezza.
Con la sottoscrizione del presente Contratto, le parti dichiarano di essersi reciprocamente comunicate oralmente tutte le informazioni previste dall'art. 13 del citato decreto legislativo n. 196 del 2003, ivi comprese quelle relative ai nominativi del responsabile e del titolare del trattamento e le modalità di esercizio dei diritti dell'interessato previste dall'art. 7 del richiamato decreto n. 196 del 2003.
Entro ... (...) giorni solari dal perfezionamento del presente Contratto verrà scambiata tra le parti una lettera con la quale l'AMM designa il Fornitore – che si impegna sin da ora ad accettare tale designazione – quale Responsabile del trattamento dei dati, individuandone oneri ed obblighi.

Per l'AMM
Per il Fornitore
....
....

Il Fornitore dichiara di avere completa conoscenza di tutte le clausole del presente Contratto, dei suoi allegati e dei documenti ivi richiamati; ai sensi e per gli effetti di cui agli articoli 1341 e 1342 cod. civ., il Fornitore dichiara di accettare tutte le condizioni e patti ivi contenuti e di avere considerato quanto stabilito e convenuto con le relative clausole. In particolare dichiara di approvare specificamente le clausole e condizioni di seguito elencate:

Articolo 1 – Oggetto del Contratto – Allegati
Articolo 2 – Durata ed efficacia
Articolo 3 – Impegni specifici del Fornitore
Articolo 5 – Ruolo del Comitato di Coordinamento e del Comitato Tecnico
Articolo 7 – Livelli di servizio e penali
Articolo 8 – Prezzi unitari, corrispettivi, modalità di pagamento e revisione prezzi
Articolo 9 – Collaudo – Verifiche
Articolo 11 – Controversie
Articolo 12 – Riservatezza
Articolo 13 – Recesso e risoluzione
Articolo 14 – Responsabilità civile
Articolo 16 – Brevetti e Diritti d'autore
Articolo 17 – Proprietà
Articolo 22 – Manleva

Il Fornitore

Appendice E: Modello di capitolato tecnico

CAPITOLATO TECNICO RELATIVO ALLA GARA PER L'ACQUISIZIONE DEL SERVIZIO DI CONTINUITÀ OPERATIVA

SOMMARIO

1. PREMESSA

In data .....le Amministrazioni:

AMM1

AMM2

AMM3

hanno stipulato un protocollo di intesa (allegato A) per l'acquisizione di servizi di Continuità Operativa. Nello stesso protocollo, le Amministrazioni hanno stabilito che l'AMM1 sia referente per il processo di gara per l'acquisizione dei servizi, fermo restando che i successivi atti contrattuali vengano stipulati da ognuna delle Amministrazioni firmatarie, che le Amministrazioni si impegnano a firmare entro e non oltre mesi uno dalla avvenuta aggiudicazione della presente gara.

2. OGGETTO DELL'APPALTO

L'appalto riguarda l'acquisizione dei seguenti servizi di Continuità Operativa:

- Servizio 1: progettazione e realizzazione della soluzione;
- Servizio 2: messa a disposizione di spazi informatici attrezzati e gestiti e dei relativi servizi di logistica e sorveglianza;

- Servizio 3: erogazione dei servizi di risorse elaborative;
- Servizio 4: erogazione dei servizi di manutenzione delle risorse elaborative (n.d.r.: eventualmente anche quelle di proprietà dell'amministrazione);
- Servizio 5: erogazione dei servizi di assistenza operativa post-realizzazione della soluzione.

3. Data di avvio dei lavori

L'avvio dei lavori deve avvenire entro e non oltre il...... .

4. Descrizione della fornitura

4.1 Obiettivi del servizio

Assicurare, per ognuna delle Amministrazioni di cui al punto 1., il corretto ripristino della disponibilità dei servizi e dei processi informatici del committente supportati da infrastrutture tecnologiche informatiche, nel caso in cui si verifichino significative interruzioni della disponibilità di queste risorse. Il ripristino si intende esteso anche ai dati individuati critici e necessari all'erogazione dei servizi ed all'operatività dei processi lavorativi.
Il ripristino deve avvenire entro le scadenze indicate in questo Capitolato per i vari servizi e processi.

4.2 Processi coperti dal servizio

Il servizio copre i seguenti processi delle Amministrazioni:

AMM1:

1) Servizio 1 – Descrizione del processo/servizio e dei dati connessi
2) Servizio 2 – Descrizione…….

……………………

AMM2:

4.3 Livelli di servizio da assicurare

Il fornitore deve garantire per le Amministrazioni committenti che l'insieme dei servizi componenti la CO permetta:

Per AMM1:

RPO pari a...

RTO pari a...

Inoltre, per i singoli servizi devono essere garantiti i seguenti livelli di servizio:

- Servizio 1: progettazione e realizzazione della soluzione
  Pronti al collaudo entro XXX giorni dalla data di efficacia contrattuale
- Servizio 2: messa a disposizione di spazi informatici attrezzati e gestiti e dei relativi servizi di logistica e sorveglianza

Garantire la corretta continuità operativa degli impianti tecnologici, con un massimo di indisponibilità di X ore/anno

- Servizio 3: erogazione dei servizi di risorse elaborative
  Esecuzione con esito positivo di X test annuali programmati, secondo le modalità descritte nell'offerta e nel rispetto di RPO e RTO sopra indicati
- Servizio 4: erogazione dei servizi di manutenzione delle risorse elaborative (n.d.r.: eventualmente anche quelle di proprietà dell'amministrazione)
  Ripristino delle apparecchiature dedicate entro X ore solari dalla richiesta, secondo le modalità convenute
- Servizio 5: erogazione dei servizi di assistenza operativa post-realizzazione della soluzione
  Garantire la segnalazione del XX,XX% degli eventi che generano degrado o blocco del servizio

Per AMM2:

…………………

Per AMM3:

…………………

4.4 Caratteristiche tecnologiche di base dei sistemi per l'operatività dei processi e servizi

I servizi e processi che dovranno essere coperti dai servizi richiesti utilizzano per il loro funzionamento nell'ambiente originale le seguenti piattaforme tecnologiche, nella configurazione descritta, che il fornitore avrà cura di riprodurre e rendere disponibili nell'ambiente di recovery:

AMM1;

AMM2;

AMM3;

....

……………………

La gestione delle variazioni delle configurazioni è regolata da quanto disposto in ogni singolo contratto di fornitura.

4.5 Specifiche di realizzazione del servizio

La Continuità Operativa (CO) è costituita dall'insieme dei servizi richiesti e dai relativi dati critici, ed ha la finalità di permettere il ripristino della disponibilità di processi e servizi delle Amministrazioni committenti in presenza di significative interruzioni del servizio di gestione operativa delle infrastrutture tecnologiche utilizzate da questi processi e servizi.
Sono incluse nel servizio le attività volte a garantire la connettività verso i servizi in questione e la sicurezza logica e fisica dei sistemi.
È inclusa nella Continuità Operativa la fornitura di tutto il materiale EDP (inclusa la carta per le stampanti) ad uso del Fornitore necessario allo svolgimento delle attività.

Al fine di permettere la corretta erogazione della CO, il fornitore presterà assistenza alle Amministrazioni committenti nello sviluppo di piani di continuità dei processi e dei servizi che verranno dalle Amministrazioni committenti ritenuti critici.
Ogni singolo Piano dovrà essere approvato dal committente entro 15 (quindici) giorni lavorativi dalla consegna dello stesso da parte del Fornitore. Ogni Amministrazione potrà richiedere modifiche ed integrazioni del piano a seguito di verifiche circa la completezza e l'adeguatezza dello stesso alle proprie necessità operative; il Fornitore dovrà predisporre tali modifiche entro quindici giorni lavorativi dalla richiesta.
Ai fini della predisposizione del piano, le attività richieste al fornitore sono:

1. analisi delle necessità;
2. analisi dell'impatto sul business per identificare le funzioni, i dati e le applicazioni critiche;
3. identificazione delle risorse minime necessarie durante un disastro, massimo tempo di indisponibilità del servizio Mainframe accettabile, impatto finanziario della perdita delle funzioni critiche e massimo intervallo temporale accettabile di disallineamento con la Produzione dei dati necessari per l'esecuzione delle funzioni stesse;
4. definizione della strategia e raccomandazione della soluzione;
5. pianificazione della gestione della crisi;
6. pianificazione della gestione delle attività in emergenza;
7. pianificazione del ripristino dei dati critici e del business in situazione di emergenza;
8. coordinamento del piano di test di Continuità Operativa;
9. manutenzione del piano organizzativo e della documentazione tecnica di ripristino;
10. training ed assistenza nell'utilizzo di tool specifici per la progettazione del piano;
11. esecuzione del piano di continuità operativa in caso di disastro;
12 ripristino del sistema di produzione entro i termini previsti.

Il Fornitore dovrà effettuare una volta ogni anno prova di ripristino della continuità di tutte le Amministrazioni committenti, allo scopo di assicurare che i piani raggiungano effettivamente gli obiettivi previsti e che vengano costantemente mantenuti allineati all'evoluzione dell'architettura e dei servizi.
Le date di effettuazione delle prove annuali dovranno essere concordate con le Amministrazioni committenti, dovranno prevedere la concomitanza di accesso da parte di tutte le Amministrazioni committenti. In ogni caso, due prove consecutive non potranno essere effettuate a meno di sei mesi solari l'una dall'altra.
Nell'ambito del servizio, il fornitore dovrà inoltre curare a regola d'arte le seguenti attività:

- asset management;
- gestione operativa infrastrutture tecnologiche e logistiche del centro di CO;
- gestione della sicurezza dei dati e delle infrastrutture;
- ....

4.6 MODALITÀ DI ATTIVAZIONE DEL SERVIZIO

Il servizio di ripristino verrà attivato a seguito di una comunicazione formale trasmessa dal, o dai, committente/i al fornitore attraverso uno dei seguenti canali:

1. e-mail: inviata dal responsabile del contratto per conto dell'amministrazione alla casella di posta BC@xxxx.it a tal fine predisposta e gestita dal fornitore, e p.c. all'indirizzo di posta elettronica del responsabile del contratto per conto del fornitore.
2. Telefono: chiamata al numero verde 800xxxxxx attivo 24 ore su 24 e attivato a cura del fornitore.

La richiesta dovrà specificare la ampiezza dell'interruzione verificatasi di disponibilità di infrastrutture, processi e servizi.
Il fornitore, non appena ricevuta la richiesta, darà immediato riscontro al, o ai, committente/i della avvenuta ricezione inviando una e-mail di risposta all'indirizzo di posta elettronica del responsabile del contratto per conto dell'amministrazione richiedente ed alla casella di posta di servizio:

- per AMM1: AMM1@AMM1.it;
- per AMM2: AMM2@AMM2.it;
- per AMM3: AMM3@AMM3.it

Entro 30 minuti dalla ricezione della richiesta il fornitore dovrà spedire ai medesimi indirizzi la previsione di tempi di ripristino.

4.7 MODALITÀ DI CHIUSURA DELLA RICHIESTA DI SERVIZIO

La esigenza di garantire la continuità operativa dei processi e servizi del committente avrà termine a seguito di una comunicazione formale trasmessa dal, o dai, committente/i al fornitore attraverso uno dei seguenti canali:

3. e-mail: inviata dal responsabile del contratto per conto dell'amministrazione alla casella di posta BC@xxxx.it a tal fine predisposta e gestita dal fornitore, e p.c. all'indirizzo di posta elettronica del responsabile del contratto per conto del fornitore.
4. Telefono: chiamata al numero verde 800xxxxxx attivo 24 ore su 24 e attivato a cura del fornitore.

La richiesta dovrà specificare la data e l'ora di termine della esigenza.
Il fornitore, non appena ricevuta la richiesta, darà immediato riscontro al, o ai, committente/i della avvenuta ricezione inviando una e-mail di risposta all'indirizzo di posta elettronica del responsabile/i del contratto per conto dell'amministrazione (delle amministrazioni) ed alle caselle di posta sopra indicate.

4.8 ORARIO DEL SERVIZIO

Il servizio è disponibile 24 ore su 24.

4.9 TEMPI DI RIPRISTINO

Il ripristino dei processi e servizi oggetto del servizio di Continuità Operativa è il seguente:

1) Servizio 1 – Ripristino entro x ore
2) Servizio 2 – Ripristino entro x ore

………….

4.10 INFRASTRUTTURE TECNOLOGICHE DEL FORNITORE

Per erogare il servizio in questione il fornitore metterà a disposizione le seguenti infrastrutture tecnologiche:

……………………

4.11 RISORSE PROFESSIONALI DEL FORNITORE

Per erogare il servizio in questione il fornitore metterà a disposizione le seguenti tipologie di risorse professionali:

……………………..

5. RIFERIMENTI STANDARD E METODOLOGICI PER LE ATTIVITÀ DEL FORNITORE

Le attività dovranno essere preferibilmente svolte in conformità ai requisiti della norma ISO 9001, alla norma ISO/IEC 27001 e alla norma ISO/IEC 20000 per le parti applicabili.
Le attività dovranno essere svolte in conformità alla metodologia di lavoro proposta dal fornitore nell'Offerta tecnica.
Per tutti i servizi richiesti in questo Capitolato, per quanto applicabile, si deve fare riferimento alle Linee Guida per la qualità dei servizi ICT pubblicate dal CNIPA, per quanto riguarda i livelli di servizio offerti e la rendicontazione da fornire all'Amministrazione riguardo i livelli di servizio effettivamente erogati.

6. PIANO DELLA QUALITÀ DEI SERVIZI

Il Piano della Qualità dei servizi dovrà essere accluso all'Offerta Tecnica.
Contiene la descrizione degli obiettivi di qualità posti ai servizi oggetto della fornitura e la descrizione delle risorse e delle tecniche, metodologie e strumenti che il fornitore adotterà per assicurare la qualità di quanto fornito.
Il Piano della Qualità costituirà il riferimento per le attività di verifica e validazione svolte dal Fornitore, all'interno dei propri gruppi di lavoro.
Ogni modifica al Piano della Qualità dovrà essere sottoposta all'approvazione delle Amministrazioni committenti, mediante le strutture previste nel protocollo di cui al punto 1.
La rilevazione delle misure necessarie a valutare il rispetto dei requisiti di qualità e dei livelli di servizio durante il periodo di validità del contratto sarà a carico del fornitore, ove non diversamente specificato. A carico del fornitore è anche la elaborazione, conservazione e presentazione delle misure, nelle modalità e nei formati che saranno di seguito indicati.

Il committente si riserva di verificare la correttezza dei metodi di rilevazione adottati e la correttezza delle misure rilevate, anche a campione.
La valutazione del rispetto dei requisiti di qualità e dei livelli di servizio è effettuata dalle Amministrazioni, che utilizzeranno a tal fine le misure rese disponibili dal fornitore. Le Amministrazioni committenti si riservano di affidare tale incarico a esperti esterni e di attivare un monitoraggio della fornitura ai sensi della normativa emessa dal CNIPA in materia.
In caso di constatazione di mancato rispetto dei requisiti di qualità dei prodotti e dei livelli di servizio, le Amministrazioni committenti applicheranno, ognuna relativamente al proprio contratto di fornitura, le penali indicate nello schema di contratto.

7. Rendicontazioni da produrre

Il fornitore dovrà produrre ogni mese, una rendicontazione sugli interventi effettuati, evidenziando:

- le richieste pervenute;
- i tempi di ripristino ed i livelli di servizio forniti;
- le attività svolte per mantenere l'allineamento delle configurazioni.

8. Responsabili del progetto

Il fornitore dovrà nominare, secondo le modalità di cui all'art. 18 dello schema di contratto, un responsabile del Progetto, il quale:

- sarà il destinatario diretto delle comunicazioni da parte delle Amministrazioni committenti ed avrà cura di trasmetterle, se necessario, agli altri soggetti che ne debbono avere conoscenza;
- sarà l'interfaccia dei responsabili dei contratti per le Amministrazioni committenti, per tutti i problemi connessi all'esecuzione del contratto e delle strutture previste nel protocollo di cui al punto 1;
- dovrà provvedere a trasmettere al, o ai, Responsabile/i del Progetto per conto delle Amministrazioni, tutte le comunicazioni che riguardano lo svolgimento delle attività previste dal contratto.

9. Durata del contratto

La durata del contratto è definita all'art. 2 dello schema di contratto.

10. Certificazioni del fornitore e monitoraggio

Al fornitore viene richiesta la certificazione ISO 9001/2000 in corso di validità alla data di pubblicazione e di chiusura del bando di Gara relativo alla gara in oggetto (OPZIONALE).
La certificazione deve coprire i processi di progettazione, sviluppo, produzione, commercializzazione, installazione ed assistenza nel settore informatico ed essere stata rilasciata

alla unità organizzativa che effettuerà operativamente le attività previste dal contratto (OPZIONALE).
Il committente si riserva la facoltà di affidare a terze parti il monitoraggio sullo svolgimento del contratto, come previsto dalla normativa vigente e dalle disposizioni emesse in merito dal CNIPA.

Appendice F: Standard e link di riferimento

Standard

Esistono standard emessi da enti nazionali, nordamericani ed europei, che sono spesso riconosciuti come riferimenti anche oltre i confini delle nazioni dove sono stati prodotti. È possibile citare:

- lo standard britannico BSI PAS 56 “Guide to Business Continuity Management”;
- lo standard americano NFPA 1600 “Standard on Disaster/Emergency Management and Business Continuity Programs – 2004 Edition”;
- lo standard prodotto dallo SPRING (“Standards, Productivity and Innovation Board”), una organizzazione di ispirazione governativa di Singapore SS507 “Singapore Standards for Business Continuity/Disaster Recovery (BC/DR) Service Providers”.

Lo standard BSI PAS 56 sta per essere convertito in uno standard BSI di più alto livello (secondo la gerarchia BSI). Si tratta dello standard BS 25999 che sarà costituito da due parti, secondo il consueto schema “should/shall”:

- BS 25999-1:2006 “Code of Practice for BCM”, che costituisce l’evoluzione del PAS 56;
- BS 25999-2:2006 “A Specification for BCM”.

Si prevede la disponibilità della prima parte per la fine del 2006 e quella della seconda parte per i primi mesi del 2007.
Particolare è lo standard prodotto dallo SPRING, che si propone di dare indicazioni a organizzazioni nella scelta di un fornitore del servizio di Continuità Operativa.
Un discorso a parte deve essere fatto per alcuni standard ISO. Pur non esistendo ad oggi uno standard specifico per la CO, le norme ISO/IEC 17799:2005 “Information technology – Security techniques – Code of practice for information security management” e la recentissima ISO/IEC 27001 “Information technology – Security techniques – Information security management systems – Requirements”, pur riguardando il processo di messa in sicurezza di un sistema informatico, anche dal punto di vista della certificazione, fanno riferimento a un sistema di CO quale requisito richiesto perché un sistema informatico sia considerato in sicurezza. Va inoltre segnalato come, nell’ambito del JTC1/SC27 dell’ISO, che si occupa di sicurezza informatica, è iniziato l’iter di produzione di uno specifico standard, che dovrebbe essere numerato ISO/IEC 27006, i cui contenuti saranno quelli di linee guida per il disaster recovery. Questo standard, che certamente recepirà in gran parte i contenuti di standard esistenti, è previsto essere disponibile entro il 2007. Da segnalare, anche se non specifiche sul tema della continuità operativa, le ondicazioni contenute nello standard ISO 20000 “Information Technology - Service Management”.

Gli standard menzionati non sono sovrapponibili e una loro analisi approfondita richiederebbe uno studio che esula dalle brevi note di questa appendice.
Nella successiva sezione dei link è possibile trovare gli indirizzi delle organizzazioni sopra citate.

Link di riferimento

Di seguito, vengono indicati alcuni link a organizzazioni pubbliche o private che trattano, anche in via esclusiva, il tema della Continuità Operativa. Sono stati esclusi link a specifici fornitori di soluzioni per la Continuità Operativa.
Sul piano nazionale, si segnalano le istituzioni bancarie (1., 2.), da sempre attente a tutti gli aspetti di garanzia della continuità dei servizi.
Sul piano europeo, si segnalano alcuni link inglesi (3., 4.), mentre per quanto riguarda organizzazioni internazionali, si segnalano l'ISO (5.), il BSI inglese (6.) e il NFPA statunitense (7.). Tutti gli altri link si riferiscono ad organizzazioni non pubbliche (ad eccezione dello SPRING, che si occupa, in generale, di migliorare il sistema produttivo di Singapore) che trattano specificatamente il tema della Continuità Operativa.

1. **Banca d'Italia www.bancaditalia.it**
2. **ABI Lab http://www.abilab.it**
3. **London Prepared Business Continuity Advice – Index http://www.londonprepared.gov.uk/business/businesscont/index.htm**
4. **UK Resilience – EP – Business Continuity http://www.ukresilience.info/preparedness/businesscontinuity/index.shtm**
5. **ISO – International Organization for Standardization http://www.iso.org**
6. **BSI – British Standard Institution http://www.bsi-global.com/**
7. **NFPA – National Fire Protection Association http://www.nfpa.org**
8. **Spring Singapore http://www.spring.gov.sg**
9. **The Business Continuity Institute http://www.thebci.org/**
10. **Contingency Planning http://www.contingencyplanning.com/**
11. **Continuity Central the worldwide business continuity and disaster recovery portal http://www.continuitycentral.com/index.htm**
12. **Continuity Forum http://www.continuityforum.org/**
13. **Continuity Insights Magazine http://www.continuityinsights.com/**
14. **Disaster Recovery Journal's – Sample Plans http://www.drj.com/new2dr/samples.htm**
15. **Disaster Recovery Journal's Homepage http://www.drj.com/**
16. **Disaster Resource http://www.disaster-resource.com/**
17. **DisasterRecoveryTools.com – The Resource for Computer Security and Data Recovery Information http://www.disasterrecoverytools.com/index.php**
18. **Disaster Recovery Planning.org http://www.drplanning.org/portal/**
19. **Global Continuity http://www.globalcontinuity.com/**
20. **INFOSYSSEC The Security Portal for Information System Security Professionals http://www.infosyssec.net/infosyssec/security/buscon1.htm**

Appendice G: Glossario

A

Access Control List (ACL)
Lista contenente regole d'accesso che determinano le possibilità di accesso dei soggetti agli oggetti di un sistema (le risorse).

Access Management
Processo di realizzazione e applicazione delle politiche di sicurezza relative all'**autorizzazione**.

Accordi di Basilea
Accordi sui requisiti patrimoniali delle banche, frutto del lavoro del Comitato di Basilea, istituito dai governatori delle Banche centrali dei dieci Paesi più industrializzati (G10).

Accreditamento
Riconoscimento formale dell'indipendenza, **affidabilità** e competenza tecnica di un **centro per la valutazione della sicurezza**.

Affidabilità
Esprime il livello di fiducia che l'utilizzatore ripone nel sistema informativo: l'utente deve potersi fidare del sistema che usa ed esso si deve comportare secondo le previsioni dell'utente.

Agente ostile
Persona o forza naturale che genera la minaccia.

Alert
Vedi **Avviso.**

Amministratore della sicurezza
Persona responsabile di attuare, controllare, e rendere effettive le regole di sicurezza stabilite dal Responsabile della sicurezza.

Analisi costi/benefici
Processo che facilita la valutazione finanziaria delle differenti opzioni strategiche del **Business Continuity Management** e confronta il costo di ciascuna opzione con i guadagni attesi.

Analisi del rischio
Attività volta a identificare minacce e vulnerabilità di un sistema allo scopo di definirne gli obiettivi di sicurezza e di permettere la gestione del rischio.

Analisi degli effetti
L'analisi della gestione con cui una organizzazione valuta gli impatti quantitativi (finanziari) e qualitativi, gli effetti e le perdite che possano risultare qualora una attività dovesse subire un **E/I/C** di Continuità Operativa.

ANS
(Autorità Nazionale per la Sicurezza). Il Presidente del Consiglio dei Ministri ovvero l'Organo dallo stesso delegato per l'esercizio delle funzioni in materia di tutela delle informazioni, documenti e materiali classificati; (DPCM 11 aprile 2002).

ANSI
Acronimo di American National Standards Institute. Istituto americano che coordina il settore privato statunitense intorno a un sistema normativo volontario e supportato dalle organizzazioni pubbliche e private.

Antispamming
Strumento di sicurezza informatica progettato per contrastare lo **spamming**.

Antivirus
Strumento di sicurezza informatica progettato per intercettare, bloccare e curare i virus informatici.

Asset
Letteralmente significa bene prezioso. Sono tutte le risorse che costituiscono il patrimonio di un'organizzazione. Ne esistono tre tipi: asset fisico (edifici, apparecchiature); asset finanziari (moneta corrente, deposito bancari ed azioni); asset intangibili (reputazione).

Appliance
Dispositivo hardware dedicato a una funzione ben precisa, in contrapposizione a un computer generico. Il router è l'esempio tipico di un appliance di rete.

Asset informativi
Costituiscono il patrimonio informativo di un'organizzazione: il know-how, la proprietà intellettuale, i brevetti, i processi produttivi, le conoscenze delle singole persone e così via.

Assurance
Vedi **Garanzia**.

Attacco
Azione o evento che può pregiudicare la sicurezza di un sistema.

Attivazione
L'implementazione delle funzionalità di Continuità Operativa, delle procedure, delle attività e piani in risposta a una emergenza di Continuità Operativa, a un Evento, un Incidente e/o una Crisi (E/I/C). Vedi: **Invocazione**.

Audit
Insieme delle attività di revisione continua del sistema dei controlli all'interno di un'organizzazione. Si pone la finalità di garantire la legalità e la legittimità delle attività dell'organizzazione.

Audit dei sistemi informativi automatizzati
Tipologia specifica di **audit** che ha per oggetto i controlli (nel senso di punti di verifica) del solo sistema informativo automatizzato.

Autenticazione
Processo di verifica dell'identità dichiarata del **soggetto**, correlato con l'identificazione. Alternativamente, può essere definito come il processo con il quale un **sistema informatico** verifica che il **soggetto**, dal quale ha ricevuto una comunicazione, è o non è l'entità che è stata dichiarata. Riferita a un messaggio di posta elettronica, è l'insieme di due componenti: autenticazione dell'origine, ovvero la garanzia che il messaggio provenga realmente dalla sorgente dichiarata, e integrità, ovvero la garanzia che il messaggio sia identico a quello inviato.

Autorizzazione
Concessione dei diritti di accesso al **soggetto** dopo che questo è stato identificato e autenticato.

Avviso
Notifica formale che un **E/I/C** è avvenuto e che possa richiedere una Gestione di **Continuità Operativa** o un'invocazione di Gestione di una Crisi.

B

Back door
Sezione di codice che permette di aggirare i normali controlli di sicurezza.

Backlog
L'effetto sulle attività dell'accumulo di lavoro che avviene come risultato della indisponibilità di sistemi o processi per un periodo ritenuto inaccettabile.

Backup
Un processo tramite il quale i dati, in formato cartaceo o elettronico, sono copiati, in modo da essere resi disponibili e utilizzati se il dato originale da cui è stata prodotta la copia è andato perduto, distrutto o corrotto.

Base dati
Vedi **Database**.

BCP
Vedi **Business Continuity Plan**.

Best practice
Migliore approccio possibile per affrontare una determinata situazione. È basato sull'osservazione di quanto fatto dalle organizzazioni leader in circostanze analoghe.

BIA
Vedi **Business Impact Analysis**.

Black list
Elenchi di domini o di specifici indirizzi di posta noti come fonte di messaggi indesiderati. Possono essere anche elenchi di URL di siti web vietati.

Bomba logica
Codice dannoso dormiente che si attiva a seguito di particolari circostanze (es. una data specifica).

BS7799
Standard del BSI per la realizzazione, valutazione e certificazione di un sistema di gestione della sicurezza delle informazioni. Consiste di due parti: la prima – diventata norma **ISO/IEC 17799** – contiene le raccomandazioni per una corretta gestione della sicurezza di sistema o di processo, mentre la seconda parte specifica i requisiti per la realizzazione di un **ISMS**. La sezione 9 tratta la Gestione della **Continuità Operativa**.

BSI
Acronimo di British Standard Institution. Ente costituito dal Dipartimento del Commercio e Industria del governo inglese con l'intento di sostenere, indirizzare e mantenere la qualità dell'industria britannica.

Business Continuity
Vedi **Continuità operativa**.

Business Continuity Plan
Vedi **Piano di continuità operativa**.

Business Continuity Management (BCM)
Un processo di gestione olistica che identifica impatti potenziali che minacciano un'organizzazione nel suo insieme e che fornisce una struttura con la capacità di offrire una risposta efficace che salvaguardi gli interessi aziendali, la sua reputazione, il marchio e le sue attività.

Business Continuity Management Programme
Un processo continuo di gestione e governo supportato dall'azienda tale da assicurare che vengano intrapresi i passi necessari atti a identificare l'impatto di perdite potenziali, a mantenere piani e strategie di recovery praticabili, ad assicurare la continuità di prodotti/servizi attraverso la pratica, la ripetizione, il test e l'addestramento relativi a procedure di manutenzione e di garanzia.

Business Impact Analysis
Vedi **Analisi degli effetti.**

Business Recovery
Vedi **Business Continuity Management**.

C

CA
Vedi **Certification Authority**.

Cavallo di Troia
Vedi **Trojan horse**.

CERT/CC
Acronimo di Computer Emergency Response Team/ Coordination Center. È il nucleo di risposta alle

emergenze di sicurezza in Internet, creato presso il Software Engineering Institute della Carnegie Mellon University, a Pittsburgh, negli USA.

Certification Revocation List
Lista dei certificati digitali revocati accessibile a chi ne deve usufruire. È mantenuta costantemente aggiornata dalla Certification Authority.

Certification Authority
Ente che gestisce il rilascio e la revoca delle chiavi per la firma digitale e i certificati digitali che contengono informazioni sul depositario della firma.

Certificato digitale
Documento informatico siglato da una Certification Authority che contiene la chiave pubblica di un individuo, le informazioni sulla sua identità e altre caratteristiche (vedi anche **X.509**).

Certificazione
L'attestazione da parte dell'organismo di certificazione che conferma i risultati della valutazione e la corretta applicazione dei criteri adottati e della relativa metodologia. Va distinta la certificazione di sistema o processo, come descritta ad esempio nello standard **ISO/IEC 17799** e la certificazione di prodotto, come descritta ad esempio nello standard **ISO 15408**.

Certificazione di sicurezza
Attestazione mediante la quale un organismo/autorità di certificazione garantisce il soddisfacimento da parte dell'oggetto certificato dei requisiti definiti in una norma di riferimento. Dipendentemente dall'oggetto della certificazione e dalla norma di riferimento utilizzata possono distinguersi vari tipi di certificazione di sicurezza: **Certificazione di sistemi/prodotti ICT**, **Certificazione di sistemi di gestione della sicurezza ICT (Information Security Management Systems – ISMS)** e **Certificazione digitale X.509.**

Certificazione di sistemi/prodotti ICT
Oggetto della certificazione può essere un intero sistema ICT installato in uno specifico ambiente, un prodotto ICT utilizzabile in una pluralità di sistemi ICT o un documento che definisce ambiente e requisiti di sicurezza per un sistema/prodotto ICT. Le norme di riferimento sono i criteri di valutazione europei **ITSEC** ed i **Common Criteria** adottati dall'**ISO/IEC (IS 15408)**. In Italia le certificazioni di questo tipo sono disciplinate dal DPCM 11 aprile 2002 e dal DPCM 30 ottobre 2003 che hanno istituito due distinti Schemi Nazionali di certificazione, il primo dei quali è utilizzabile esclusivamente ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello stato.

Certificazione di sistemi di gestione della sicurezza ICT (Information Security Management Systems – ISMS)
Oggetto della certificazione è il processo mediante il quale un'organizzazione gestisce la sicurezza ICT al suo interno. La norma di riferimento è rappresentata dallo standard britannico **BS7799**, la cui parte introduttiva, non utilizzabile ai fini della certificazione, è stata adottata dall'**ISO/IEC (IS 17799)**. In Italia il Sincert (Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione e Ispezione) ha sviluppato uno Schema per l'accreditamento di organismi di certificazione ai quali viene affidato il compito di verificare il soddisfacimento dei requisiti contenuti nella norma.

Certificazione digitale X.509
Oggetto della certificazione è l'associazione di una **chiave** pubblica di cifratura e di altre informazioni a un soggetto titolare. La certificazione viene emessa da un'autorità di certificazione sotto forma di un documento, denominato **certificato digitale**, strutturato secondo lo standard **X.509**.

CeVa
Acronimo di Centro di Valutazione. Sono i laboratori omologati dall'**ANS** per la valutazione di prodotti e sistemi di sicurezza secondo lo schema nazionale.

Chiave
Nei sistemi di cifratura è un valore variabile utilizzato da un algoritmo, per cifrare dati.

Cifratura
Tecnica usata per proteggere dati in chiaro codificandoli, in modo da renderli incomprensibili a chi non deve vederli.

Classificazione dei dati
Processo di analisi e attribuzione dei livelli di criticità ai dati, in riferimento a parametri di integrità, riservatezza e disponibilità.

Client/Server
Gruppo di computer collegati da una rete di comunicazione in cui il client pone richieste e il server le esegue. L'elaborazione può avvenire sia sul client che sul server, ma comunque in maniera trasparente per gli utenti.

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

Codice dannoso
Vedi **Codice maligno**.

Codice maligno
Programma o parti di un programma che interferisce con le normali operazioni di un computer e viene eseguito senza il consenso dell'utente. Esempi classici sono i **virus** e i **Trojan horse**.

Cold site
Centro di elaborazione d'emergenza che dispone dei componenti e delle infrastrutture elettriche di un sistema di produzione normale, ma non contiene i computer. Il sito è pronto per accogliere i computer quando occorre passare dal centro di calcolo principale a quello di riserva, in caso di disastro.

Comitato di gestione della crisi (o Comitato di crisi)
Organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività degli altri gruppi

coinvolti nella continuità operativa. Tra i suoi compiti: l'approvazione del piano di continuità operativa, la dichiarazione dello stato di crisi, l'avvio delle attività di rientro alle condizioni normali, i rapporti con l'esterno e le comunicazioni ai dipendenti.

Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni
Comitato istituto con Decreto interministeriale (Min. comunicazioni e Min. innovazione e tecnologie) del 24 luglio 2002, avente funzioni di indirizzo e coordinamento delle iniziative in materia di sicurezza nelle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni. Nell'aprile 2004 il Comitato ha pubblicato le "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la Pubblica Amministrazione".

Common Criteria
Standard internazionale di valutazione della sicurezza in ambito informatico nato con l'obiettivo di rilasciare nuovi criteri per un mercato informatico sempre più articolato e globale.

Computer forensic
Vedi **Forensics**.

Content filtering
Strumenti di sicurezza informatica che analizzano il grado di pericolosità dei contenuti dei file scaricati da Internet o degli allegati di posta elettronica, eliminando questi oggetti se potenzialmente dannosi.

Content security management
Sistemi di gestione della sicurezza dei contenuti. Sono evoluzioni e integrazioni degli **antivirus** e dei sistemi **antispamming**. Analizzano anche i file scaricati da Internet e le pagine dei siti web visitati.

Continuità operativa
Insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il **Disaster Recovery**.

Controllo
Nell'accezione derivata dalla lingua inglese identifica una contromisura. Nell'accezione classica italiana, significa invece punto di verifica di un'attività, di un sistema e così via.

Controllo accessi
Funzione di sicurezza volta a controllare che un utente possa espletare le sole operazioni di propria competenza.

Contromisura
Strumento di natura tecnologica, organizzativa o fisica, atto a contrastare un **attacco** nei confronti di un sistema.

Coordinatore emergenza
La persona assegnata al ruolo di coordinamento delle attività di evacuazione di un sito e/o di un edificio dotato di servizi di emergenza regolamentari.

Copia dei dati
Un processo con cui dati ritenuti critici vengono copiati in un'altra locazione, in modo che non vengano persi nell'evento di perdita di **Continuità Operativa**. Può essere utilizzata come soluzione di **Disaster Recovery** effettuando la copia remotamente. Esistono funzioni di copia dati a livello hardware e a livello software.

Cost Benefit Analysis
Vedi **Analisi costi/benefici.**

Cracker
Chiunque irrompa in un **sistema informatico** con intenti vandalistici, con l'intenzione cioè di provocare dei danni al sistema stesso al fine di comprometterne il funzionamento. Vedi anche **Hacker**.

Crisi
Un evento o una percezione che minaccia le operazioni, il personale, il valore dell'azienda, il nome, la reputazione e/o gli obiettivi strategici di una organizzazione.

Crisis Management Plan
Vedi **Piano di Gestione Crisi.**

Crisis Management Team
Vedi **Unità di crisi.**

Crittografia
Metodo per memorizzare e trasmettere dati in una forma tale affinché una persona o un sistema, diversi dal destinatario, siano impossibilitati a leggerli o processarli.

Crittografia a chiave asimmetrica
Vedi **Crittografia a chiave pubblica**.

Crittografia a chiave pubblica
Metodo di crittografia che si basa su una coppia di numeri digitali matematicamente correlati. Uno dei due è definito chiave privata (riservata al proprietario), l'altro numero è chiamato chiave pubblica (disponibile a chiunque). Ciò che viene cifrato con la chiave pubblica può essere decifrato solo con la chiave privata corrispondente. È denominato anche Crittografia a chiave asimmetrica.

Crittografia a chiave segreta
Metodo di crittografia che si basa su una stessa chiave singola segreta, usata sia per cifrare sia per decifrare. È denominato anche Crittografia a chiave simmetrica.

Crittografia a chiave simmetrica
Vedi **Crittografia a chiave segreta**.

CRL
Vedi **Certificate Revocation List**.

Cross certification
Relazione di mutua fiducia tra differenti **Certification Authority**, ottenuta con lo scambio e il riconoscimento biunivoco di certificati emessi da ognuna.

CSIRT
Acronimo di Computer Security Incident Response Team. Vedi **Incident Response Team**.

CSO
Acronimo di Chief Security Officer. Vedi **Responsabile della sicurezza**.

Custode dei dati
Colui che protegge e gestisce i processi e i relativi dati nel rispetto della sicurezza e dei livelli di servizio concordati.

D

DPCM 16 gennaio 2002
Decreto contenente indicazioni per le pubbliche amministrazioni statali in materia di sicurezza informatica e delle telecomunicazioni. Riporta in allegato uno schema di autovalutazione dello stato della sicurezza informatica e l'organizzazione a cui le PA devono tendere per realizzare una "base minima di sicurezza".

DAC
Vedi **Discretionary Access Control**.

Danno
Effetto che può essere prodotto da una minaccia.

Database
Collezione di dati registrati e correlati tra loro.

Database Replication
Duplicazione parziale o totale dei dati da un **database** sorgente a uno o più **database** destinatari. Il processo di replicazione può utilizzare svariate metodologie (**data mirroring**) e può essere eseguito in modalità sincrona, asincrona o a tempi specifici, a seconda delle tecnologie utilizzate, dei requisiti di recupero richiesto, della distanza e della connettività esistente verso il **database** sorgente. La replicazione, se eseguita remotamente, può funzionare come **backup** per situazioni catastrofiche e altri **outage** di grandi entità.

Data Mirroring
Vedi **Copia dei dati.**

Dati sensibili
Ai sensi del Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati personali
Ai sensi del Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dato
Rappresentazione oggettiva di un fatto o evento che consenta la sua trasmissione oppure interpretazione da parte di un soggetto umano o uno strumento informatico.

DDOS
Acronimo di Distributed Denial Of Service. **Attacco** DOS di grandi dimensioni, proveniente da numerosi computer e diretto a uno o più computer, al fine di saturarli.

Decifratura
Tecnica usata per ricostruire i dati originali, precedentemente cifrati, in modo da renderli comprensibili. La decifratura è l'operazione inversa alla cifratura.

DeMilitarized Zone
(DMZ) Piccola rete di computer posta in una zona neutrale localizzata fra una rete privata e una rete esterna, pubblica o non fidata. I servizi che la rete privata dovrebbe rendere pubblici sono collocati proprio sui computer della DMZ. In questo modo, alla rete esterna viene impedito l'accesso alla rete privata.

Denial Of Service
Tipo di **attacco** volto a saturare le capacità di elaborazione di uno o più sistemi target il cui scopo è quello di produrre una perdita di funzionalità, più o meno prolungata nel tempo.

DES
Acronimo di Data Encryption Standard. Algoritmo di crittografia a chiave segreta basato su una chiave a 56 bit.

Directory
Database gerarchico usato per memorizzare dati gestibili tramite appositi protocolli (per esempio l'LDAP: Light Directory Access Protocol).

Disaster Recovery
Insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.

Disaster Recovery Plan
Documento di progettazione e pianificazione delle attività di **Disaster Recovery**.

Disastro
Una calamità improvvisa e non pianificata che causa gravi danni o perdite. Tipicamente implica l'inizio del trasferimento dal sito primario ad una località secondaria.

Discretionary Access Control
Controllo accessi discrezionale: il proprietario di un oggetto può a sua discrezione stabilire chi può avere accesso alle proprie risorse.

Disponibilità
Requisito di sicurezza che esprime la protezione dall'impossibilità di utilizzo di un'informazione o risorsa.

DMZ
Vedi **DeMilitarized Zone**.

Documento Programmatico per la Sicurezza
Documento richiesto all'art. 34 del Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" il cui contenuto è specificato nell'allegato B, punto 19, relativo al trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici.

Dominio dell'emergenza
Insieme delle misure e delle attività che hanno lo scopo di assicurare, nel caso di eventi disastrosi, il ripristino della normalità operativa. Vedi anche **Business Continuity** e **Disaster Recovery**.

Dominio della prevenzione
Insieme delle misure di sicurezza volte alla protezione preventiva di un sistema informativo automatizzato. Vedi anche Sistema di protezione.

Dominio delle emergenze contingenti
Insieme delle misure di sicurezza che consentono di reagire ai malfunzionamenti e agli incidenti. Vedi anche **Gestione degli incidenti**.

DOS
Vedi **Denial Of Service**.

DPS
Vedi **Documento Programmatico per la Sicurezza**.

DRP
Vedi **Disaster Recovery Plan**.

E

Emergenza
Una situazione reale o incombente (tanto da rappresentare una minaccia), che possa causare lesioni, morti, distruzione di proprietà e/o interruzione delle normali attività operative di una azienda.

ENISA
European Network and Information Security Agency, Agenzia consultiva dell'Unione europea avente lo scopo di raggiungere un alto livello di sicurezza ICT nella Comunità europea.

E/I/C
Evento, Incidente, Crisi.

Evacuazione
Lo spostamento di impiegati, visitatori e lavoratori temporanei da un sito e/o un edificio a un luogo sicuro in maniera controllata e monitorata in caso di un **E/I/C**.

Exploit
Attacco finalizzato a produrre accesso a un sistema o incrementi di privilegio.

F

Fallback
Altro termine per indicare una alternativa. Ad esempio, il sito di fallback è un altro sito/edificio che può essere utilizzato qualora il sito/edificio originario divenga inusabile o indisponibile.

Fiducia
Vedi **Affidabilità**.

Firewall
Strumento progettato per impedire accessi non autorizzati a reti private da reti aperte e viceversa, quindi posto come barriera tra le due.

Firma digitale
Particolare tipo di **firma elettronica qualificata** basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Firma elettronica
Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Firma elettronica qualificata
Firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca del firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

Forensics
Disciplina che si occupa della preservazione, identificazione ed estrazione dei dati, dello studio e della documentazione dei computer, per evidenziare le prove a scopo di indagine.

Funzione di sicurezza
Vedi **Contromisura**.

G

Gap Analysis
Un sondaggio il cui obiettivo è identificare le differenze tra i requisiti del **Business Continuity Management** (quanto il processo indica sia necessario in casi di **E/I/C**) e quanto sia effettivamente disponibile.

Garante italiano per la privacy
Organo che opera al fine di garantire, tra l'altro, il rispetto della disciplina in materia di trattamento dei dati personali.

Garanzia
Fiducia nella capacità di un sistema di protezione di soddisfare i requisiti di sicurezza.

Gateway
Dispositivo hardware o software che traduce due protocolli diversi fra loro. In altri casi, viene chiamato gateway qualsiasi meccanismo che fornisce l'ac-

cesso a un altro sistema. Ad esempio, un router è un gateway che permette a una rete locale di accedere a Internet.

Gestione degli incidenti
Insieme delle attività, dei processi e procedure, dell'organizzazione e delle misure di sicurezza volte al rilevamento, alla risposta e alla risoluzione degli incidenti di sicurezza.

Gestione del rischio
Attività volta a individuare le contromisure logiche, fisiche, organizzative e amministrative per soddisfare gli obiettivi di sicurezza e contrastare i rischi individuati dall'**analisi del rischio**.

Governo della sicurezza
Vedi **Security governance**.

H

Hacker
Chiunque irrompa in un **sistema informatico** con l'intento di scoprirne il funzionamento e la struttura, o di ottenere informazioni riservate contenute all'interno del sistema stesso. Vedi anche **Cracker**.

Hash
Stringa di caratteri a lunghezza fissa ricavata dal testo del messaggio secondo appositi algoritmi; consente, per comparazione successiva, di verificare se il messaggio pervenuto al destinatario è corrispondente all'originale.

Honeypot
Sistema che si presta volutamente a subire attacchi di malintenzionati al fine ottenere informazioni utili a fronteggiare le azioni dei malintenzionati stessi.

Host-based IDS
IDS che si occupano di individuare le potenziali intrusioni e le azioni sospette sui server e i computer in generale.

Hot site
Un sito di riserva (centro di elaborazione dati, area di lavoro) che fornisce funzioni di **Business Continuity Management** equipaggiato con hardware e software, interfacce per le telecomunicazioni e uno spazio controllato in grado di fornire supporto di elaborazione dati alternativo in tempi relativamente immediati per mantenere le attività critiche dell'organizzazione. Pronto all'uso in caso di evento catastrofico al centro primario.

HTTPS
Acronimo di Secure Hyper Text Transmission Protocol. È un protocollo sviluppato allo scopo di cifrare e decifrare le pagine web che vengono inviate dal server ai client.

I

Identificazione
Atto per cui un soggetto dichiara di essere se stesso; è il primo passo dell'**autenticazione**.

ICANN (Internet Corporation for Assigned Names and Numbers)
Ente no-profit, organizzato in sede internazionale, avente la responsabilità di assegnare gli indirizzi IP (Internet Protocol) e l'identificatore di protocollo e di gestire il sistema dei nomi a dominio di primo livello (Top-Level Domain) generico (gTLD) e del codice internazionale (ccTLD) nonché i sistemi di root server. Questi servizi erano inizialmente prestati su mandato del governo degli Stati Uniti da IANA (Internet Assigned Numbers Authority, a cui ICANN si è ora sostituito, e da altri enti.

IDS
Vedi **Intrusion Detection System**.

IEC
Acronimo di International Electrotechnical Commission. È l'organismo normatore su scala mondiale nel campo elettrico ed elettrotecnico; prepara le norme tecniche che vengono adottate nei paesi maggiormente industrializzati.

IEEE
Acronimo di Institute of Electrical and Electronics Engineers. È un istituto che comprende tecnici e ricercatori di tutto il mondo interessati al settore elettrotecnico e elettronico.

IETF
Acronimo di Internet Engineering Task Force. Ente che emette gli standard per Internet, noti come RFC (Request For Comment).

Incident Response Team
Gruppo di esperti preposto a ricevere segnalazioni di incidenti e a intervenire per risolverli.

Incidente (di sicurezza)
Attività dannosa che ha come obiettivo la compromissione dei requisiti di sicurezza del sistema informativo automatizzato o di una sua parte.

Informazione
Interpretazione e significato assegnato a uno o più dati.

Informazione classificata
Ogni informazione, documento o materiale cui sia stata attribuita, da un'autorità competente, una classifica di segretezza; (DPCM 11 aprile 2002).

Infrastruttura
Un edificio e tutti i servizi ad esso di supporto. Una infrastruttura può essere tecnologica (computer, cavi, impianti telefonici) e strutturale (edifici, servizi, impianti di condizionamento).

Infrastruttura a chiave pubblica
Piattaforma di tecnologie e servizi basata su un sistema di crittografia a chiavi asimmetriche per la gestione dei certificati digitali e servizi correlati.

Infrastruttura Critica
Sistemi la cui indisponibilità o distruzione avrebbe un impatto debilitante sulla sicurezza economica di una organizzazione, di una comunità, di una nazione.

Integrità
Requisito di sicurezza che esprime la protezione da modifiche non autorizzate alle informazioni.

Interessato
Persona fisica, giuridica, ente o associazione cui si riferiscono dati personali.

Intrusion Detection System
Strumento per individuare tentativi d'**attacco** alla rete o più in generale alterazioni delle configurazioni dei sistemi in rete.

IPSec
Versione sicura del protocollo IP. Consente di realizzare un canale sicuro tra due elementi che comunicano tramite una rete.

IRT
Vedi **Incident Response Team**.

ISMS
Acronimo di Information Security Management System. Vedi Sistema di gestione della sicurezza delle informazioni.

ISO
Acronimo di International Organization for Standardization. Organismo fondato nel 1946 responsabile della creazione degli standard internazionali in molti settori, tra cui elaboratori e trasmissione dei dati. ISO è una federazione non governativa a cui partecipano circa 130 enti normatori internazionali.

ISO/IEC 17799
Information technology – Code of practice for information security management, codice di condotta per la gestione della sicurezza dell'informazione di un'organizzazione.

ISO/IEC 15408
Vedi **Common Criteria**.

ISO/IEC TR 13335
Technical Report dell'ISO contenente le Guidelines for the Management of IT Security (GMITS).

ISSO
Acronimo di Information System Security Officer. Vedi **Responsabile della sicurezza**.

Istituto Superiore delle Comunicazioni (ISCOM)
Organo tecnico-scientifico che opera nell'ambito del Ministero delle comunicazioni. La sua attività riguarda fondamentalmente i servizi alle imprese, la normazione, la sperimentazione e la ricerca di base e applicata, la formazione e l'istruzione specializzata nel campo delle telecomunicazioni.

ITSEC
Insieme strutturato di criteri per la valutazione della sicurezza IT di prodotti e sistemi pubblicato da paesi europei. È l'acronimo di Information Technology Security Evaluation Criteria.

ITSEM
Acronimo di Information Technology Security Evaluation Manual. È il manuale che definisce la metodologia da applicare nelle valutazioni secondo i criteri ITSEC e fornisce le basi per un'unificazione dei metodi di valutazione della sicurezza definiti dai vari enti valutatori.

L

Laboratorio per la valutazione della sicurezza
L'organizzazione indipendente che ha ottenuto l'accreditamento e che pertanto è abilitata a effettuare valutazioni e a fornire assistenza, come definita nell'ambito dello Schema Nazionale istituito con DPCM 30/10/2003.

Livello di servizio
Indicatore che traduce le attese qualitative in obiettivi quantitativi misurabili, sulla base dei quali è possibile verificare il rispetto delle clausole contrattuali e in particolare dei livelli di qualità pattuiti.

Log
File o altro documento elettronico che registra informazioni dettagliate sugli eventi di un sistema, di solito nella stessa sequenza in cui si verificano.

Logic bomb
Vedi **Bomba logica**.

Logon
Atto di collegarsi a un elaboratore. Tipicamente richiede che si digiti un identificativo utente (user-id) e una password su un computer.

LVS
Acronimo che identifica i **Laboratori di Valutazione della Sicurezza**.

M

MAC
Vedi **Mandatory Access Control**.

Malicious code
Vedi **Codice maligno**.

Mandatory Access Control
Modello di controllo accessi dove il proprietario non può stabilire in completa autonomia e totale libertà le regole di accesso, dando luogo anche a situazioni di anarchia. La decisione se concedere o meno un certo tipo di accesso a una risorsa è intrapresa in funzione delle politiche di sicurezza, ovviamente tenendo conto delle esigenze del proprietario.

Meccanismi di sicurezza
Strumenti, apparati, software, algoritmi e procedure organizzative e operative che realizzano le funzioni di sicurezza.

MIME
Multipurpose Internet Mail Extensions, standard Internet che specifica come gli allegati ai messaggi devono essere formattati in modo da poter essere scambiati tra sistemi di posta differenti.

Minaccia
Potenziale pericolo che può causare dei danni ai beni di un'organizzazione in funzione dell'esistenza di vulnerabilità.

Misura di sicurezza
Vedi **Contromisura**.

Modello organizzativo sulla sicurezza ICT
Nel contesto della Pubblica Amministrazione, rappresenta l'architettura nazionale in termini di strutture e responsabilità sulla sicurezza ICT, capace di sviluppare linee guida, raccomandazioni, standard e tutte le procedure di certificazione.

N

NAT
Acronimo di Network Address Translation. Consiste nel nascondere gli indirizzi IP interni a una rete privata, mostrando all'esterno un unico indirizzo pubblico, in genere quello del firewall.

Network-based IDS
IDS che si occupa di individuare le potenziali intrusioni e le azioni sospette in rete.

NIST
Acronimo di National Institute of Standards and Technologies. Ente del Dipartimento del Commercio del governo USA che emette standard e linee guida in ambito IT per il governo federale.

Non ripudio
Capacità di un sistema di crittografia di rendere impossibile all'autore di un messaggio o più in generale di un documento elettronico di disconoscerne la paternità.

NSA
Acronimo di National Security Agency. Ente del governo statunitense per le attività di spionaggio e controspionaggio in ambito civile, molto attivo nell'ambito della ricerca e sviluppo su tematiche di sicurezza e crittografia.

O

Obiettivi di sicurezza
Esigenza di protezione da determinati attacchi contro i dati e le risorse del sistema informativo automatizzato.

OCSE
Acronimo di Organizzazione per la Cooperazione e lo Sviluppo Economico. Vedi **OECD**.

OCSI
Acronimo che identifica l'Organismo di Certificazione della Sicurezza Informatica nell'ambito dello **Schema Nazionale** italiano

OCSP
Acronimo di On-line Certificate Status Protocol, sistema usato per il controllo in tempo reale dei certificati digitali revocati.

OECD
Acronimo di Organization for Economic Co-Operation and Development. Nota anche come OCSE, è l'organizzazione internazionale con 30 paesi membri per la promozione del buon governo nel settore pubblico e privato.

Oggetto
Nell'ambito della sicurezza delle informazioni rappresenta un'entità passiva, anche materiale (come una stampante), che contiene informazioni.

Oggetto della valutazione (ODV)
Il sistema o prodotto sottoposto alla valutazione.

One-time password
Password dinamica che cambia a ogni logon.

Open source
Si intende un processo di produzione, distribuzione ed evoluzione del software che si basa sull'apertura del codice sorgente e sulla sua libera circolazione.

Open System Interconnections
Standard internazionale per l'organizzazione di reti, definito dall'ISO e dal IEEE nei primi anni '80.

Operational Level Agreement
Accordo interno fra due o più entità di un'organizzazione che definisce le responsabilità di tutte le componenti dell'organizzazione. Un OLA vincola queste componenti a precise definizioni dei servizi e/o delle forniture in termini di qualità e quantità che possono essere richieste e fornite.

Orange Book
Volume delle Rainbow Series che riporta lo standard **TCSEC**.

Organismo di certificazione
Organismo che sovrintende alle attività operative di valutazione e certificazione nell'ambito dello **Schema nazionale**.

Organizzazione
Un'impresa, un'entità corporativa; un'azienda, un'entità pubblica o governativa, un dipartimento, un'agenzia; un affare, un ente di carità.

OSI
Vedi **Open Systems Interconnection**.

Outage
Periodo di tempo in cui un servizio, un sistema, un processo o una funzione operativa è inaccessibile o inusabile, comportando un alto impatto sull'organizzazione, compromettendo il raggiungimento degli obiettivi operativi dell'organizzazione stessa. L'outage è diverso dal "downtime", in cui fermi di processo o di sistema avvengono come parte della normale operatività, e il cui l'impatto riduce semplicemente l'efficienza a breve termine dei processi.

Outsourcing
Il trasferimento delle funzioni operative a un fornitore indipendente, esterno o interno.

P

Pacchetto
Blocco di dati oggetto di trasmissione. Un pacchetto contiene sia i dati sia le informazioni per l'indirizzamento.

Packet filtering
Tecnica di controllo del traffico implementata da uno strumento di sicurezza di rete, di solito router o firewall, che permette o impedisce le comunicazioni sulla base delle informazioni di livello 3 e 4 della pila ISO OSI, contenute nei pacchetti.

Parametri di sicurezza
Vedi **Requisiti di sicurezza**.

Parola chiave
Vedi **Password**.

Password
Stringa di caratteri, generalmente cifrata dall'elaboratore, che autentica un utente a un sistema.

Patrimonio Informativo
Insieme delle informazioni di un'organizzazione.

PDCA
Acronimo di Plan-Do-Check-Act. Modello dei sistemi di gestione articolato attraverso le fasi della definizione, realizzazione, esercizio, monitoraggio, revisione, manutenzione e miglioramento continuo dei processi.

Penetration test
Attività preventiva volta a individuare eventuali vulnerabilità nei dispositivi hardware e software di una rete. Eseguire un penetration test significa cercare di violare il perimetro di difesa ricorrendo a tecniche di hacking.

PGP
Acronimo di Pretty Good Privacy. È un programma di crittografia scritto da Phillip Zimmerman. Permette la cifratura di messaggi di posta e file tramite l'uso di sistemi di crittografia asimmetrici e simmetrici.

Phishing
Tecnica di "adescamento informatico" a fini truffaldini. Consiste nell'indurre utenti di Internet a fornire dati personali, utilizzabili, per esempio, per accrediti di denaro verso terzi, presentandosi sulla rete in modo apparentemente legittimo.

Piano della sicurezza
Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito, in genere, di una organizzazione.

Piano di continuità operativa
Documento di progettazione e pianificazione delle attività di continuità operativa, contenente le misure di carattere operativo da adottare per attuare le gestione della situazione di **emergenza** crisi e il successivo ripristino della normale operatività.

Piano Nazionale sulla Sicurezza
Nel contesto della Pubblica Amministrazione, rappresenta il piano che definisce attività, responsabilità, tempi per l'introduzione degli standard e delle metodologie necessarie per pervenire alla certificazione di sicurezza.

PIN
Acronimo di Personal Identification Number. Un tipo di password. Ha la forma di numero segreto assegnato a una persona che, assieme ad altri modi per identificarla, serve a verificarne l'autenticità. I PIN sono stati impiegati dal circuito Bancomat.

PKI
Vedi **Public Key Infrastructure**.

Politiche di sicurezza
Costituiscono l'insieme dei principi, norme, regole, consuetudini che regolano la gestione delle informazioni di una organizzazione in termini di protezione e distribuzione. Si possono classificare in politiche di alto livello e funzionali.

Privacy
Tratta la riservatezza in merito alle informazioni riguardanti un soggetto. In Italia il concetto di privacy è disciplinato dal Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

Profilo di protezione
Il documento che descrive per una certa categoria di **ODV** e in modo indipendente dalla realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente ed i requisiti funzionali e di fiducia, definiti secondo i Common Criteria.

Proprietario dei dati
Colui che ha la responsabilità dei processi che utilizzano e gestiscono i dati di propria competenza, incluso la relativa classificazione.

Protocollo
Regole secondo cui una rete funziona e controlla flusso e priorità nelle trasmissioni.

Proxy Server
Server che agisce prendendo il posto di un utente. I tipici proxy ricevono una richiesta di collegamento da un utente, e stabiliscono se l'utente o l'indirizzo IP corrispondente possono usarne i servizi. In caso di successo, attiva un collegamento a destinazione remota al posto dell'utente.

Public Key Infrastructure
Vedi **Infrastruttura a chiave pubblica**.

R

RA
Vedi **Registration Authority**.

RBAC
Vedi **Role-Based Access Control**.

Recovery
Vedi **System recovery**.

Recovery Site
Vedi **Sito di recovery**.

Registration Authority
Autorità di registrazione in una PKI; chiede i certificati digitali alla propria CA dopo aver acquisito tutte le informazioni necessarie all'identificazione del titolare del certificato.

Requisiti di sicurezza
Esprimono ciò che si intende per sicurezza: riservatezza, integrità e disponibilità.

Responsabile del trattamento
Ai sensi del Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Responsabile della sicurezza
Persona responsabile per stabilire e far attuare le regole di sicurezza. Risponde all'Alta Direzione.

RFC
Acronimo di Request For Comment. Sono gli standard dei protocolli, degli algoritmi e dei sistemi usati in ambito Internet.

Ripristino
Attività che consiste nel riportare un sistema al suo stato precedente a un errore. Nel caso di perdita di dati, permette di rigenerarli come erano prima dell'evento, in genere partendo da un backup.

Rischio
Possibilità che un determinato evento avverso causi un danno a un bene, sfruttandone i punti deboli. Di solito si misura combinando l'impatto e la probabilità di accadimento. In senso generale può essere definito come la minaccia di una azione o una non-azione che potrebbe impedire a una organizzazione il raggiungimento degli obiettivi operativi.

Riservatezza
Requisito di sicurezza che esprime la protezione da divulgazione non autorizzata delle informazioni.

Risk Analysis
Vedi **Analisi del rischio.**

ROI
Acronimo di Return On Investment. Ritorno sugli investimenti effettuati. In ambito sicurezza, si parla anche di ROSI, cioè Return On Security Investment.

Role-Based Access Control
Modello di controllo accessi basato sul concetto di ruolo: consente di attribuire le autorizzazioni attraverso la semplice assegnazione di un ruolo a un soggetto.

RSA
Algoritmo di crittografia a chiave pubblica usato sia per la cifratura sia per l'**autenticazione**. Deriva dalle iniziali dei cognomi dei suoi ideatori: R. Rivest, A. Shamir e L. Adleman.

Ruoli e responsabilità
Definisce la categoria delle funzioni organizzative all'interno di un'organizzazione per la sicurezza che hanno lo scopo di specificare le figure operative che pianificano e gestiscono il sistema di protezione evidenziando le responsabilità e le attività di loro competenza.

S

S/MIME
Versione sicura del protocollo **MIME** che permette di includere nei normali messaggi di posta elettronica anche file di grafica, audio e altro.

SAN
Vedi **Storage Area Network**.

Salvaguardia
Contromisure e azioni da intraprendere per ridurre il livello di vulnerabilità di un bene nei confronti di una minaccia. Possono essere tecniche e fisiche, ma anche gestionali e organizzative (politiche e direttive).

Schema Nazionale
Insieme delle procedure e delle regole nazionali necessarie per la valutazione e certificazione di sicurezza relativa a sistemi/prodotti ICT, in conformità ai criteri europei ITSEC o agli standard internazionali ISO/IEC IS-15408 (*Common Criteria*). Nell'ambito di uno Schema Nazionale esiste un unico Organismo di certificazione che accredita un certo numero di Laboratori di Valutazione della Sicurezza ai quali è affidato il compito di verificare il soddisfacimento delle norme di riferimento.

Security appliance
Apparati di sicurezza che racchiudono in un unico box hardware più strumenti di sicurezza: ad esempio **IDS**, **firewall** e **antivirus**.

Security governance
Vedi **Sistema di gestione della sicurezza delle informazioni**.

Security log correlation
Sistema di sicurezza capace di raccogliere i log, normalizzarli (riconducendoli a un formato comune, anche se provenienti dai diversi strumenti) e correlarli opportunamente, consentendo di rilevare intrusioni e di evitare falsi positivi.

Security manager
Vedi **Responsabile della Sicurezza**.

Security Operation Center
Centro operativo di gestione della sicurezza.

Service Level Agreement
Accordo sul **livello di servizio** che un utente chiede a un fornitore. È regolato da uno specifico contratto.

SGSI
Vedi **Sistema di gestione della sicurezza delle informazioni**.

Sicurezza delle reti e dell'informazione
Capacità di una rete o di un **sistema informatico** di resistere ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettano la disponibilità l'**integrità** e la **riservatezza** dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema.

Sicurezza delle informazioni
Disciplina nell'ambito della tutela del patrimonio di un'organizzazione, orientata a garantire la protezione degli **asset informativi**.

Sicurezza informatica
Branca della sicurezza delle informazioni che si occupa principalmente della protezione del sistema informatico dal punto di vista tecnologico.

Sicurezza perimetrale
Protezione del perimetro o bordo esterno di una rete privata mediante tecnologie di sicurezza informatica.

Single Point of Failure
L'unico erogatore di un servizio, di una attività e/o processo, senza alternative, la cui perdita possa condurre alla perdita totale di una attività critica per l'**organizzazione**.

Single Sign-On
Sistema volto a semplificare le operazioni di accesso alle applicazioni evitando all'utente la ripetizione delle proprie credenziali.

Sistema biometrico
Dispositivi che utilizzano sofisticate tecnologie di comparazione tra una caratteristica fisica dell'individuo e la precedente registrazione elettronica di questa parte.

Sistema di controllo accessi
Insieme delle misure di sicurezza che hanno lo scopo di indicare i metodi e le tecnologie per regolare l'accesso alle risorse ai soli soggetti autorizzati.

Sistema di controllo o sistema dei controlli
Insieme dei controlli (intesi come punti di verifica) presenti nei processi e nei sistemi di un'organizzazione. È l'oggetto dell'**audit**.

Sistema di gestione della sicurezza delle informazioni
Parte del sistema di gestione del sistema informativo di un'organizzazione basato sul rischio per definire, realizzare, esercitare, monitorare, mantenere e migliorare il processo di sicurezza delle informazioni.

Sistema di protezione
Insieme delle misure tecnologiche, fisiche e organizzative progettato e realizzato organicamente con il fine di proteggere un sistema informativo automatizzato.

Sistema informatico
Insieme delle tecnologie informatiche a supporto dell'automazione del **sistema informativo**.

Sistema informativo
Insieme delle attività di elaborazione manuale e automatizzata dei dati, dei processi informativi, delle relative risorse umane e tecnologiche e dell'infrastruttura fisica di riferimento.

Sistema informativo automatizzato
Sistema informativo che utilizza sistemi informatici per l'elaborazione delle informazioni.

Sito duplicato (ridondato)
Sito alternativo, anche condiviso con un'altra realtà. A differenza dell'**hot site,** è un sito sempre attivo. Anche conosciuto come **Sito di Recovery**.

Sito di recovery
Sito mantenuto in stato di allerta e utilizzato in situazioni di mantenimento della **Continuità Operativa.**

SLA
Vedi **Service Level Agreement**.

Soggetto
Nell'ambito della sicurezza delle informazioni rappresenta un'entità attiva che richiede l'accesso a un oggetto o ai dati in esso contenuti.

Spam
Tentativo improprio di impiegare uno o più indirizzi di posta elettronica, allo scopo di inviare un messaggio a un gran numero di destinatari, senza che ciò sia stato espressamente richiesto.

Spammer
Creatore di **spam**.

Spamming
L'azione di creare **spam**.

SPC
Sistema Pubblico di Connettività (artt. 73 e segg. del D.Lgs 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale"); è definito come l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della Pubblica Amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.

Spoofing
Genericamente indica una tecnica di sostituzione o di falsificazione di identità, che può essere realizzata a vari livelli: IP spoofing, web spoofing, mail spoofing, ecc. aventi in comune l'uso di un falso elemento di identificazione (l'indirizzo IP, la simulazione di un sito web, una falsa identità di posta elettronica, ecc.).

SSE-CMM
Acronimo di Systems Security Engineering – Capability Maturity Model. Metodologia adottata dalla NSA e standard ISO dal 2002 con l'identificazione ISO/IEC 21827.

SSL
Acronimo di Secure Socket Layer. È un protocollo che consente, grazie a tecniche di crittografia, il trasferimento di dati tramite la rete Internet in modo sicuro.

Stateful packet inspection
Particolare tipo di tecnologia usata dai firewall che eseguono un filtro dinamico dei pacchetti di rete. Questi firewall ispezionano anche il contenuto del pacchetto e non solamente le informazioni relative all'origine e alla destinazione. Inoltre conservano una tabella contenente le informazioni dello stato di ogni connessione.

Statement of Applicability
Documento che contiene l'elenco dei controlli **BS7799** selezionati per un particolare ISMS, corredato delle motivazioni di inclusione o esclusione delle singole contromisure. Esso viene presentato al valutatore se si vuole intraprendere l'iter di certificazione secondo la norma **BS7799**-2:2002.

Storage Area Network
Rete ad alta velocità che consente di creare delle connessioni dirette tra i dispositivi hardware di memorizzazione dei dati e i server connessi in rete.

Supplier
Una persona o una azienda che fornisce beni o servizi all'**organizzazione**.

System Downtime
Interruzione pianificata o non pianificata nella disponibilità del sistema.

System Recovery
Le procedure per ripristinare un sistema computerizzato alla situazione in cui sia in grado di ricevere dati e servire applicazioni.

T

TCP/IP
Acronimo di Transmission Control Protocol/Internet Protocol. È una famiglia di protocolli di comunicazione corrispondenti ai livelli 3 e 4 della pila ISO OSI. TCP-IP è la base di Internet.

TCSEC
Acronimo di Trusted Computer System Evaluation Criteria. Definisce i criteri di valutazione di sicurezza IT, individuati dal Dipartimento della Difesa (DoD) statunitense.

Test
Una attività in cui vengano seguite alcune parti di un piano di **Continuità Operativa** per assicurarsi che il piano contenga le informazioni appropriate per produrre i risultati attesi. Un test si differenzia da un'esercitazione in quanto un test si effettua presso un sito alternativo, mentre una esercitazione è generalmente una simulazione.

Timestamp
Marca temporale ottenuta tramite apposizione della firma digitale di un documento elettronico. Serve a garantirne la certezza dell'esistenza in una certa forma e a un certo istante.

Titolare del trattamento
Ai sensi del Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Token
Dispositivo elettronico e portatile di **autenticazione**: può essere a forma di tessera magnetica.

Tracciabilità
Azione continua di registrazione delle azioni svolte da un soggetto identificato univocamente; il termine inglese corrispondente è accountability.

Trap door
Codice non documentato inserito in un programma per creare una vulnerabilità sfruttabile successivamente.

Trattamento dei dati personali
Ai sensi del Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Triple-DES
Variazione del DES, cifra il testo in chiaro 3 volte.

Trojan horse
Codice non autorizzato, in genere dannoso, nascosto di proposito in un programma, il cui utilizzo è invece autorizzato.

Tunneling
Sistema che sfrutta Internet come elemento di una VPN. Il tunnel è il percorso protetto che un certo messaggio o pacchetto può seguire su Internet.

U

Unità di Crisi
Un definito numero di ruoli e responsabilità per realizzare l'organizzazione del **Piano di Gestione Crisi**.

UPS (Uninterruptible Power Supply)
Una fonte di energia alternativa che fornisce continuità di energia per apparecchiature critiche nell'evento in cui la fornitura di energia principale divenga indisponibile.

URL
Acronimo di Uniform Resource Locator. Metodo standard per definire l'indirizzo di qualsiasi risorsa su Internet nell'ambito del World Wide Web (WWW). Ad esempio, http://www.abcdefghi.it.

URL filtering (blocking)
Strumenti di sicurezza informatica che analizzano il grado di pericolosità degli URL e delle corrispondenti pagine Web che si intende visitare, negando l'accesso se potenzialmente dannosi o se i contenuti sono vietati.

User provisioning
Sistemi per la gestione dell'intero ciclo di vita dell'utente in termini di creazione, modifica e revoca del suo codice d'identità con relativa password e abilitazione di accesso alle risorse necessario per operare.

User-id
Codice identificativo personale con cui un utente si presenta a un sistema informatico. La user-id dichiara l'identità dell'utente, la verifica della password corrispondente costituisce invece la prova di autenticità di quest'identità.

Utilizzatore dei dati
Utilizza processi e relativi dati in base alle proprie mansioni e nel rispetto delle modalità e delle autorizzazioni individuate dal proprietario e delle politiche di gestione di un'organizzazione.

V

Valutazione
L'analisi di un sistema, prodotto, profilo di protezione o traguardo di sicurezza condotta in base a predefiniti criteri applicati secondo una predefinita metodologia.

Virtual Private Network
Connessione di rete equivalente a un link dedicato ma che avviene su una rete condivisa, utilizzando una tecnica denominata tunneling.

Virus
Codice che se eseguito può inserirsi a sua volta in altri programmi e propagarsi ad altri computer via rete o tramite dischi. Quando è attivo interferisce con le normali operazioni di un sistema computerizzato. Esistono diverse tipologie di virus.

VPN
Vedi **Virtual Private Network**.

Vulnerabilità
Debolezza intrinseca di un componente del sistema informativo automatizzato che può essere sfruttata da una minaccia per arrecare un danno ai beni di un'organizzazione.

Vulnerability assessment
Attività che ha come obiettivo la valutazione del livello di protezione e dell'efficacia dei sistemi di sicurezza adottati e quindi di prevenire eventuali attacchi basati su quelle vulnerabilità.

W

Warm site
A differenza dell'**hot site**, è un sito alternativo che non prevede un'infrastruttura completa. La configurazione include di solito le connessioni alle reti, le unità disco, le unità nastro ma non i computer.

Worm
Programma che **installa** copie di se stesso su computer in rete e si moltiplica.

X.509
Standard ITU che definisce la **PKI** e il **certificato digitale** con i suoi relativi attributi.